

10/615,768

2 633

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月12日

出 願 番 号

Application Number:

特願2002-204676

[ ST.10/C ]:

[ JP 2002-204676 ]

出 願 人

Applicant(s):

株式会社東芝

2003年 2月28日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎

出証番号 出証特2003-3011817

【書類名】 特許願

【整理番号】 13789401

【提出日】 平成14年 7月12日

【あて先】 特許庁長官殿

【国際特許分類】 H04B 7/26

【発明の名称】 送信装置、受信装置及び無線基地局

【請求項の数】 16

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
研究開発センター内

    【氏名】 磯 崎 宏

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
研究開発センター内

    【氏名】 斉 藤 健

【発明者】

    【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝 府中事業所  
内

    【氏名】 加 藤 拓

【特許出願人】

    【識別番号】 000003078

    【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号

    【氏名又は名称】 株式会社 東 芝

【代理人】

    【識別番号】 100075812

    【弁理士】

    【氏名又は名称】 吉 武 賢 次

【選任した代理人】

    【識別番号】 100088889

【弁理士】

【氏名又は名称】 橘 谷 英 俊

【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信装置、受信装置及び無線基地局

【特許請求の範囲】

【請求項 1】

著作権保護が必要なコンテンツを、ネットワークを介して 1 以上の受信装置に送信する送信装置において、

前記コンテンツの蓄積または生成を行うコンテンツ供給部と、

前記受信装置と通信を行う場合の通信モードを選択する通信処理部と、

前記通信処理部にて選択された前記通信モードに基づいて、通信を行う前記受信装置の数を決定し、この受信装置の数以下の前記受信装置と認証及び鍵交換を行う認証・鍵交換処理部と、

前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、

前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備したことを特徴とする送信装置。

【請求項 2】

前記通信モードは、IEEE802.11で規定されるインフラストラクチャモードとアドホックモードとを含むことを特徴とする請求項 1 に記載の送信装置。

【請求項 3】

前記認証・鍵交換処理部は、前記インフラストラクチャモードが選択された場合には、前記アドホックモードが選択された場合よりも、認証及び鍵交換を行う前記受信装置の数を多くすることを特徴とする請求項 2 に記載の送信装置。

【請求項 4】

著作権保護が必要なコンテンツを、無線基地局を介してネットワーク経由で 1 以上の受信装置に送信する送信装置において、

前記コンテンツの蓄積または生成を行うコンテンツ供給部と、

前記無線基地局との間での認証処理に用いる前記無線基地局のネットワーク ID を予め記録する ID 記録部と、

前記 ID 記録部に記録された前記ネットワーク ID を用いて前記無線基地局を認

証する I D 認証処理部と、

前記 I D 認証処理部の認証結果に基づいて、通信を行う前記受信装置の数を切り替え、この受信装置の数以下の前記受信装置と認証及び鍵交換を行う認証・鍵交換処理部と、

前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、

前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備したことを特徴とする送信装置。

【請求項 5】

前記認証・鍵交換処理部は、前記 I D 認証処理部が認証に成功した場合には、認証に失敗した場合よりも、認証及び鍵交換を行う前記受信装置の数を多くすることを特徴とする請求項 4 に記載の送信装置。

【請求項 6】

一以上の前記無線基地局のネットワーク ID を登録するとともに、一度登録したネットワーク ID を変更できないようにする基地局 I D 登録部を備え、

前記 I D 認証処理部は、前記基地局 I D 登録部に登録されたネットワーク ID に基づいて認証を行うことを特徴とする請求項 4 又は 5 に記載の送信装置。

【請求項 7】

前記認証・鍵交換処理部及び前記 I D 認証処理部の少なくとも一方での認証に失敗した場合には、前記コンテンツの送信を禁止する送信禁止部を備え、

前記 I D 認証処理部は、前記無線基地局との間での前記ネットワーク ID の認証を所定期間ごとに繰り返し行い、

前記送信禁止部は、前記 I D 認証処理部が前記ネットワーク ID の認証に一度でも失敗すると、前記コンテンツの送信を中断することを特徴とする請求項 4 及至 6 のいずれかに記載の送信装置。

【請求項 8】

著作権保護が必要なコンテンツを、ネットワークを介して 1 以上の受信装置に送信する送信装置において、

前記コンテンツの蓄積または生成を行うコンテンツ供給部と、

前記受信装置との間で通信を行う場合の通信モードを選択する通信処理部と、  
前記通信処理部にて選択された前記通信モードに基づいて、有限回数のコピーを許可する鍵又はコピーを禁止する鍵のいずれかを使用するかを決定し、前記受信装置との間で著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、

前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、

前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備したことを特徴とする送信装置。

【請求項 9】

著作権保護が必要なコンテンツを、無線基地局を介してネットワーク経由で 1 以上の受信装置に送信する送信装置において、

前記コンテンツの蓄積または生成を行うコンテンツ供給部と、

前記無線基地局との間での認証処理に用いるネットワーク ID を記録する ID 記録部と、

前記無線基地局との間で前記ネットワーク ID の認証を行う ID 認証処理部と、

前記 ID 認証処理部の認証結果に基づいて、有限回数のコピーを許可する鍵とコピーを禁止する鍵とのいずれかを使用するかを決定し、前記受信装置との間で著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、

前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、

前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備したことを特徴とする送信装置。

【請求項 10】

前記認証・鍵交換処理部は、

前記有限回数のコピーを許可する鍵を使用して通信を行なう前記受信装置の数を制限することを特徴とする請求項 8 または 9 に記載の送信装置。

【請求項 11】

前記認証・鍵交換処理部は、前記 ID 認証処理部が認証に成功した場合には有

限回数のコピーを許可する鍵を選択し、前記 I D 認証処理部が認証に失敗した場合にはコピーを禁止する鍵を選択することを特徴とする請求項 8 または 9 に記載の送信装置。

【請求項 1 2】

コンテンツの送信を禁止するべき前記受信装置の識別情報を登録したりボケーション情報登録部を備え、

前記認証・鍵交換処理部は、前記リボケーション情報登録部に登録されている前記受信装置との間では、認証を行わないことを特徴とする請求項 1 または 1 1 のいずれかに記載の送信装置。

【請求項 1 3】

コンテンツの送信を禁止するべき前記無線基地局の識別情報を登録したりボケーション情報登録部を備え、

前記 I D 認証処理部は、前記リボケーション情報登録部に登録されている前記無線基地局との間では、認証を行わないことを特徴とする請求項 4、5、6、7 及び 9 のいずれかに記載の送信装置。

【請求項 1 4】

著作権保護が必要なコンテンツを、送信装置からネットワーク経由で受信する受信装置において、

前記送信装置との間で通信を行う場合の通信モードを選択する通信処理部と、  
前記通信処理部にて選択された前記通信モードに基づいて、有限回数のコピーを許可する鍵又はコピーを禁止する鍵を前記送信装置との間で交換し、前記送信装置との間で、著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、

前記送信装置から暗号化された前記コンテンツを受信するネットワークインタフェース部と、

前記ネットワークインタフェース部で受信した前記コンテンツを前記認証・鍵交換処理部で交換された鍵を用いて復号を行う復号処理部とを具備したことを特徴とする受信装置。

【請求項 1 5】

著作権保護が必要なコンテンツを、送信装置から無線基地局を介してネットワーク経由で受信する受信装置において、

前記無線基地局との間での認証処理に用いるネットワークIDを記録するID記録部と、

前記無線基地局との間で前記ネットワークIDの認証を行うID認証処理部と、

前記ID認証処理部の認証結果に基づいて、有限回数のコピーを許可する鍵とコピーを禁止する鍵とのいずれか一方を選択して前記送信装置との間で交換し、この送信装置との間で、著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、

前記送信装置から暗号化された前記コンテンツを受信するネットワークインタフェース部と、

前記ネットワークインタフェース部で受信した前記コンテンツを前記認証・鍵交換処理部で交換された鍵を用いて復号を行う復号処理部とを具備したことを特徴とする受信装置。

#### 【請求項 1 6】

著作権保護が必要なコンテンツを、送信装置からネットワーク経由で受信し、受信したコンテンツを1以上の受信装置に送信する無線基地局において、

前記送信装置との間で前記ネットワークIDの認証を行う第1のID認証処理部と

、

前記受信装置との間で前記ネットワークIDの認証を行う第2のID認証処理部と

、

コンテンツの送信を禁止すべき前記送信装置の識別情報とコンテンツの受信を禁止すべき前記受信装置の識別情報との少なくとも一方を登録したりボケーション情報登録部と、を備え、

前記送信装置及び前記受信装置は、前記第1及び第2のID認証処理部の認証結果に基づいて、認証及び鍵交換を行う前記送信装置または前記受信装置の数または暗号化の方式を切り替えることを特徴とする無線基地局。

#### 【発明の詳細な説明】

#### 【0 0 0 1】



【発明の属する技術分野】

本発明は、著作権保護が必要な各種のコンテンツをネットワーク経由で送受信する送信装置、受信装置及び無線基地局に関する。

【0002】

【従来の技術】

近年、IEEE802.11等の規格に準拠した無線機器が低価格になったこともあり、無線通信システムを簡易かつ安価に構築できるようになった。また、無線通信システムの通信速度も高速化する傾向にあり、通信ケーブルを用いた有線通信と速度的にあまり差がなくなりつつある。

【0003】

最近では、AVコンテンツ等の大容量データを家庭用のコンピュータで手軽に扱えるようになってきたため、無線通信システムでAVコンテンツ等を送受信できれば、ユーザにとって好都合である。

【0004】

【発明が解決しようとする課題】

しかしながら、DVDプレーヤ等のAVコンテンツ再生装置の再生信号を電波で送信すると、所定範囲内のAVコンテンツ受信装置すべてで受信できてしまう。このため、著作権保護を図るべく、認証に成功したAVコンテンツ受信装置のみがAVコンテンツを受信できるような仕組みが考えられる。ところが、いったんAVコンテンツ受信装置にて著作権保護レイヤでの認証が成功してしまうと、そのAVコンテンツ受信装置が正式に許可を得た装置か否かを区別できないという問題がある。

【0005】

このような問題を回避するために、無線環境においても、正式に許可を得た機器以外の無線機器が許可なくアクセスするのを防止し、安全な著作権保護を実現する無線通信システムが提案されている（公開番号P2002-14304）。

【0006】

ところが、利用者Aが機器に対して自分の所有物であることを示すIDを設定して機器に対するアクセスコントロールの設定をしたとしても、別の機器所有者B

がそのIDを知ってしまえば、利用者Aの無線機器にアクセスできてしまう。このため、悪意のあるコンテンツ所有者が無線通信システムを構築し、機器のIDを公開してしまえば、著作権保護のかかったコンテンツを著作権者の許可なしに配布することが可能となる。従って、著作権保護の観点からするとコンテンツの不正流通を防ぐための根本的な解決にはならない。

#### 【 0 0 0 7 】

本発明は、このような点に鑑みてなされたものであり、その目的は、ユーザの使い勝手を悪くすることなく、著作権保護強化を図れる送信装置、受信装置及び無線基地局を提供することにある。

#### 【 0 0 0 8 】

##### 【課題を解決するための手段】

上述した課題を解決するために、本発明は、著作権保護が必要なコンテンツを、ネットワークを介して1以上の受信装置に送信する送信装置において、前記コンテンツの蓄積または生成を行うコンテンツ供給部と、前記受信装置と通信を行う場合の通信モードを選択する通信処理部と、前記通信処理部にて選択された前記通信モードに基づいて、通信を行う前記受信装置の数を決定し、この受信装置の数以下の前記受信装置と認証及び鍵交換を行う認証・鍵交換処理部と、前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備する。

#### 【 0 0 0 9 】

また、著作権保護が必要なコンテンツを、無線基地局を介してネットワーク経由で1以上の受信装置に送信する送信装置において、前記コンテンツの蓄積または生成を行うコンテンツ供給部と、前記無線基地局との間での認証処理に用いる前記無線基地局のネットワークIDを予め記録するID記録部と、前記ID記録部に記録された前記ネットワークIDを用いて前記無線基地局を認証するID認証処理部と、前記ID認証処理部の認証結果に基づいて、通信を行う前記受信装置の数を切り替え、この受信装置の数以下の前記受信装置と認証及び鍵交換を行う認証・鍵交換処理部と、前記認証・鍵交換処理部で交換された鍵を用いて前記コンテ

ンツの暗号化を行う暗号処理部と、前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備する。

#### 【0010】

また、著作権保護が必要なコンテンツを、ネットワークを介して1以上の受信装置に送信する送信装置において、前記コンテンツの蓄積または生成を行うコンテンツ供給部と、前記受信装置との間で通信を行う場合の通信モードを選択する通信処理部と、前記通信処理部にて選択された前記通信モードに基づいて、有限回数のコピーを許可する鍵又はコピーを禁止する鍵のいずれかを使用するかを決定し、前記受信装置との間で著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備する。

#### 【0011】

また、著作権保護が必要なコンテンツを、無線基地局を介してネットワーク経由で1以上の受信装置に送信する送信装置において、前記コンテンツの蓄積または生成を行うコンテンツ供給部と、前記無線基地局との間での認証処理に用いるネットワークIDを記録するID記録部と、前記無線基地局との間で前記ネットワークIDの認証を行うID認証処理部と、前記ID認証処理部の認証結果に基づいて、有限回数のコピーを許可する鍵とコピーを禁止する鍵とのいずれかを使用するかを決定し、前記受信装置との間で著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、前記認証・鍵交換処理部で交換された鍵を用いて前記コンテンツの暗号化を行う暗号処理部と、前記暗号処理部において暗号化された前記コンテンツを前記受信装置に送信するネットワークインタフェース部とを具備する。

#### 【0012】

また、著作権保護が必要なコンテンツを、送信装置からネットワーク経由で受信する受信装置において、前記送信装置との間で通信を行う場合の通信モードを選択する通信処理部と、前記通信処理部にて選択された前記通信モードに基づい

て、有限回数のコピーを許可する鍵又はコピーを禁止する鍵を前記送信装置との間で交換し、前記送信装置との間で、著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、前記送信装置から暗号化された前記コンテンツを受信するネットワークインタフェース部と、前記ネットワークインタフェース部で受信した前記コンテンツを前記認証・鍵交換処理部で交換された鍵を用いて復号を行う復号処理部とを具備する。

#### 【0013】

また、著作権保護が必要なコンテンツを、送信装置から無線基地局を介してネットワーク経由で受信する受信装置において、前記無線基地局との間での認証処理に用いるネットワークIDを記録するID記録部と、前記無線基地局との間で前記ネットワークIDの認証を行うID認証処理部と、前記ID認証処理部の認証結果に基づいて、有限回数のコピーを許可する鍵とコピーを禁止する鍵とのいずれか一方を選択して前記送信装置との間で交換し、この送信装置との間で、著作権保護のための認証及び鍵交換を行う認証・鍵交換処理部と、前記送信装置から暗号化された前記コンテンツを受信するネットワークインタフェース部と、前記ネットワークインタフェース部で受信した前記コンテンツを前記認証・鍵交換処理部で交換された鍵を用いて復号を行う復号処理部とを具備する。

#### 【0014】

また、著作権保護が必要なコンテンツを、送信装置からネットワーク経由で受信し、受信したコンテンツを1以上の受信装置に送信する無線基地局において、前記送信装置との間で前記ネットワークIDの認証を行う第1のID認証処理部と、前記受信装置との間で前記ネットワークIDの認証を行う第2のID認証処理部と、コンテンツの送信を禁止すべき前記送信装置の識別情報とコンテンツの受信を禁止すべき前記受信装置の識別情報との少なくとも一方を登録したりボケーション情報登録部と、を備え、前記送信装置及び前記受信装置は、前記第1及び第2のID認証処理部の認証結果に基づいて、認証及び鍵交換を行う前記送信装置または前記受信装置の数または暗号化の方式を切り替える。

#### 【0015】

#### 【発明の実施の形態】

以下、本発明に係る送信装置、受信装置及び無線基地局について、図面を参照しながら具体的に説明する。

【0016】

(第1の実施形態)

図1は本発明に係る送信装置、受信装置及び無線基地局を含む無線通信システムの第1の実施形態の全体構成を示すブロック図である。図1の無線通信システムは、DVDプレーヤ等のコンテンツ再生機能とコンテンツを送信する無線インタフェースとを有する無線機器（以下、ソース機器）1と、ソース機器1から送信されたコンテンツを無線基地局2を介して受信する無線機器（以下、シンク機器）3とを備えている。これらソース機器1、無線基地局2及びシンク機器3は、ローカルエリア無線ネットワークAに接続されている。

【0017】

図1に示すように、ローカルエリア無線ネットワークAとは別のローカルエリア無線ネットワークBが形成され、このネットワークBには、ソース機器1と同様の機能を持つ無線機器（以下、ソース機器）4と、無線基地局2と同様の機能を持つ無線基地局5とが接続されている。

【0018】

ここで、シンク機器3がローカルエリア無線ネットワークBに接続可能な範囲に移動する場合について考える。「移動」とは、必ずしも物理的な移動にかかわらず、設定の変更によって所属するネットワークを変更する場合も含むものとする。

【0019】

すなわち、シンク機器3は、無線基地局2が形成するネットワークAと無線基地局5が形成するネットワークBのどちらにも接続可能な範囲内に位置しているものと仮定する。また、ソース機器1、無線基地局2及びシンク機器3は同一人物（A氏とする）の所有物であり、ソース機器4と無線基地局5は同一人物（B氏とする）の所有物であるとする。

【0020】

図1では、ソース機器1とシンク機器3が無線基地局2とそれぞれ直接無線通

信を行う場合を想定しているが、ソース機器 1 とシンク機器 3 が無線通信機能を持たず、ソース機器 1 とシンク機器 3 に有線で接続される不図示のブリッジ機器が無線基地局 2 と無線通信を行う場合や、ソース機器 1 とシンク機器 3 が無線通信機能を持つが、ブリッジ機器を介して無線基地局 2 と無線通信を行う場合にも適用可能である。

## 【 0 0 2 1 】

ここで、コンテンツとは、例えばMPEG4データのような動画データや音声データを指し、著作権保護をかけた上で送信すべきものを対象とする。ソース機器 1 が送信するコンテンツはA氏の所有物であり、A氏が私的利用に限りコピーまたは閲覧できるものとする。同様に、ソース機器 4 が送信するコンテンツはB氏の所有物であり、B氏が私的利用に限りコピーまたは閲覧でき、A氏はB氏が許可しないにかかわらず、B氏の所有するコンテンツをコピーまたは閲覧することは許されないものとする。

## 【 0 0 2 2 】

なお、ここでは、ローカルエリア無線ネットワークとしてIEEE802.11を仮定して説明する。IEEE802.11は、無線LANの一種であり、現在多くのPCに搭載されており、今後は様々なAV機器に搭載されることが期待されている（例えば <http://www.ieee802.org/11> にて取得可能に開示されている文書に説明が詳しい）。

## 【 0 0 2 3 】

以下、図 1 のような状況において、利用者Aの所有するシンク機器 3 が、同じく利用者Aの所有する無線基地局 2 を介してソース機器 1 からのみコンテンツを受信可能であり、利用者Bの所有する無線基地局 5 を介してソース機器 4 への接続を制限し、同時にB氏の所有するソース機器 4 がA氏の所有するシンク機器 3 にコンテンツを送信することを制限するための構成について説明する。

## 【 0 0 2 4 】

図 2 は無線基地局 2, 5 の内部構成の一例を示すブロック図である。図 2 に示すように、無線基地局 2, 5 は、IEEE802.11物理レイヤ処理を実行する802.11インターフェース処理部 1 1 と、IEEE802.11データリンクレイヤ処理を実行する802.11通信処理部 1 2 と、DTCPネットワークIDを記録するDTCPネットワークID記録

部 1 3 とを有する。

【 0 0 2 5 】

DTCPネットワークIDは、製造者または販売者等が製造時または販売時に機器に対して一意に定めた値であり、所有者はこの値を知ることができるが、変更はできない。

【 0 0 2 6 】

図 3 はソース機器 1, 4 の内部構成の一例を示すブロック図である。図 3 に示すように、ソース機器 1, 4 は、コンテンツを蓄積するコンテンツ蓄積部 2 1 と、コンテンツ蓄積部 2 1 からコンテンツを読み出してIEEE802.11パケットに変換するパケット処理部 2 2 と、著作権保護の処理を行うDTCP認証・鍵交換処理部 2 3 と、送信データを暗号・復号化するDTCP暗号・復号処理部 2 4 と、IEEE802.11データリンクレイヤ処理を実行する802.11通信処理部 2 5 と、IEEE802.11物理レイヤ処理を実行する802.11インターフェース処理部 2 6 と、DTCPネットワークIDの値を変更するDTCPネットワークID入力部 2 7 と、DTCPネットワークIDを記録するDTCPネットワークID記録部 2 8 と、DTCPネットワークIDの認証を行うDTCPネットワークID認証処理部 2 9 と、を有する。

【 0 0 2 7 】

DTCPネットワークIDの初期値は、製造者または販売者等が定めた値である。DTCPネットワークID記録部 2 8 は、記録可能なDTCPネットワークIDの数を一定数に制限する機能を持つ。

【 0 0 2 8 】

ここで、DTCPとは、Digital Transmission Contents Protectionの略であり、IEEE1394やUSB等でデファクトスタンダードとなっている著作権保護方式である。この方式は、著作権保護が必要なAVデータなどのコンテンツに対して送信機器と受信機器との間で認証・鍵交換を行い、AVデータを暗号化して転送する仕組みを持つ（例えば<http://www.dttla.com>にて取得可能に開示されている文書に説明が詳しい）。

【 0 0 2 9 】

図 4 はシンク機器 3 の内部構成の一例を示すブロック図である。図 4 に示すよ

うに、シンク機器 3 は、パケットをディスプレイなどに出力するための処理を行なうコンテンツ再生処理部 3 1 と、基地局から受信した IEEE802.11 パケットをコンテンツデータに変換するパケット処理部 3 2 と、著作権保護の処理を行う DTCP 認証・鍵交換処理部 3 3 と、送信データを暗号・復号化する DTCP 暗号・復号処理部 3 4 と、IEEE802.11 データリンクレイヤ処理を実行する 802.11 通信処理部 3 5 と、IEEE802.11 物理レイヤ処理を実行する 802.11 インターフェース処理部 3 6 と、DTCP ネットワーク ID の値を変更する DTCP ネットワーク ID 入力部 3 7 と、DTCP ネットワーク ID を記録する DTCP ネットワーク ID 記録部 3 8 と、DTCP ネットワーク ID の認証を行う DTCP ネットワーク ID 認証処理部 3 9 と、を有する。

#### 【 0 0 3 0 】

ここで重要なのは、DTCP ネットワーク ID 入力部 2 7 及び 3 7 である。上述したように、無線基地局 2 に記録されている DTCP ネットワーク ID は書き換えることができない。一方、ソース機器 1 とシンク機器 3 は DTCP ネットワーク ID 入力部 2 7 及び 3 7 によって DTCP ネットワーク ID を任意の値に変更可能である。しかし、DTCP ネットワーク ID 入力部 2 7 及び 3 7 には変更回数を記録するためのレジスタが設けられており、一定回数以上の DTCP ネットワーク ID の変更はできない。この仕組みにより、利用者はネットワーク ID の変更回数が制限される。

#### 【 0 0 3 1 】

図 5 は本実施形態の無線通信システムの処理手順を示す図である。まず、シンク機器 3 と無線基地局 2 との間で DTCP ネットワーク ID 認証を行う（ステップ S 1）。この認証に成功すると、シンク機器 3 はソース機器 1 に対して DTCP 認証要求を行う（ステップ S 2）。

#### 【 0 0 3 2 】

この要求を受けて、ソース機器 1 と無線機器 2 との間で DTCP ネットワーク ID 認証を行う（ステップ S 3）。次に、ソース機器 1 とシンク機器 3 との間で DTCP 認証・鍵交換を行う（ステップ S 4）。その後、ソース機器 1 は、鍵交換した鍵を使って暗号化したコンテンツを無線基地局 2 を介してシンク機器 3 に送信する（ステップ S 5）。

#### 【 0 0 3 3 】



図 6 はシンク機器 3 の処理手順を示す図である。まず、利用者は無線基地局 2 と同一の DTCP ネットワーク ID をシンク機器 3 の DTCP ネットワーク ID として予め登録しておく（ステップ S 1 1）。

【 0 0 3 4 】

次に、DTCP ネットワーク ID の更新回数記録レジスタの値が所定値未満か否かを判定し（ステップ S 1 2）、所定値以上であれば、DTCP ネットワーク ID を変更できないため、所定のエラー処理を行なう（ステップ S 1 3）。

【 0 0 3 5 】

更新回数記録レジスタの値が所定値未満であれば、DTCP ネットワーク ID の値を変更し、変更回数記録レジスタの値を増やす（ステップ S 1 4）。これらの一連の処理を DTCP ネットワーク ID 登録処理と呼ぶ。

【 0 0 3 6 】

なお、シンク機器 3 の DTCP ネットワーク ID の値が無線基地局 2 の値と同一であれば、ステップ S 1 1 ～ S 1 4 の処理は不要である。

【 0 0 3 7 】

次に、コンテンツの送受信処理を開始する。まず、DTCP 認証・鍵交換を行なう前に、無線基地局 2 の DTCP ネットワーク ID とシンク機器 3 の DTCP ネットワーク ID の値が一致するか否かの相互認証処理を行なう（ステップ S 1 5）。この認証は、認証鍵として DTCP ネットワーク ID の値を使い、ISO/IEC 9798-2 で定められたような共通鍵認証方式を使えばよい。また、DTCP ネットワーク ID に署名をつけて相互に送信し、受信側の機器がその署名を検証することで、DTCP ネットワーク ID が一致するか否かを検証してもよい。

【 0 0 3 8 】

無線リンクレイヤでパケットが確実に改竄されておらず、シンク機器 3 から無線基地局 2 に送られたものであることが保証されれば、暗号化を伴う認証処理は必ずしも必要ではなく、単純に無線基地局 2 に対して DTCP ネットワーク ID の値を送信するだけでもよい。以下、この手順をまとめて DTCP ネットワーク ID 認証と呼ぶ。

【 0 0 3 9 】

DTCPネットワークID認証が成功した場合（ステップS 1 6）、ソース機器1はシンク機器3に対してDTCP認証・鍵交換要求を送信し（ステップS 1 7）、DTCPネットワークID認証が失敗した場合はエラー処理を行う（ステップS 1 8）。

#### 【0 0 4 0】

図7は図6のステップS 1 8のエラー処理手順を示す図である。エラー処理には例えば、（1）DTCP認証を中断する方法（ステップS 2 1）や、（2）コピー制限のレベルを変更する方法（ステップS 2 2）などが考えられる。

#### 【0 0 4 1】

（1）の場合、ソース機器に対して何も送信しない方法や、DTCP認証要求を拒否するエラーメッセージを送信する方法などがある。（2）の場合、例えばDTCPには、伝送されるデータに対して著作権保持者によるコピーの制限を規定するために、CCIと呼ばれる複数のレベルが規定されている。このレベルには、コピーを禁止するCopy Never及びNo More Copiesと、一世代に限りコピーを認める Copy One Generationと、コピーを自由に認める Copy Freeとがある。利用者がシンク機器に対してCopy One Generationでコンテンツを受信するように指定したとしても、シンク機器が無線基地局とDTCPネットワークIDの認証に失敗した場合は、コピーの制限を厳しくしたCopy NeverやNo More Copiesでコンテンツを受信するようにシンク機器に要求する。

#### 【0 0 4 2】

図8はソース機器1の処理手順を示す図である。図8に示すように、ソース機器1にも、無線基地局2と同一のDTCPネットワークIDを登録しておく（ステップS 3 1）。シンク機器3からDTCP認証・鍵交換の要求を受信する（ステップS 3 2）と、ソース機器1は無線基地局2とDTCPネットワークIDの値が一致するか相互認証処理を行なう（ステップS 3 3）。この認証も、前述したシンク機器3と無線基地局2の際に用いた認証と同様の手順で行なえばよい。

#### 【0 0 4 3】

次に、この認証に成功したか否かを判定し（ステップS 3 4）、成功した場合はシンク機器3とDTCP認証・鍵交換処理を行い（ステップS 3 5）、失敗した場合はエラー処理を行う（ステップS 3 6）。

## 【 0 0 4 4 】

なお、このDTCPネットワークIDの認証に先立ち、IEEE802.11iのような無線リンクレイヤでの認証・鍵交換と暗号化によるデータの秘匿と検証処理を行っても良い。

## 【 0 0 4 5 】

図9は図8のステップS36のエラー処理手順を示す図である。エラー処理には例えば、(1)シンク機器3から受信したDTCP認証要求を破棄し、DTCP認証処理を終了させる方法(ステップS41)、(2)コピー制限のレベルを変更する方法(ステップS42)、(3)コンテンツを配布するシンク機器の台数を制限する方法(ステップS43)、(4)上記の(2)と(3)の全部又は一部を併用する方法など種々の方法などが考えられる。

## 【 0 0 4 6 】

(1)の場合、シンク機器3に対してDTCP認証要求を拒否するエラーメッセージを送信する方法や、応答そのものをしない方法がある。(2)の場合、例えば、シンク機器3がソース機器1に対してCopy One Generationでコンテンツを要求したとしても、ソース機器1が無線基地局2とDTCPネットワークIDの認証に失敗した場合、コピーの制限を厳しくしたCopy NeverやNo More Copiesでコンテンツを送信する。(3)の場合、例えばDTCPにはDTCP認証・鍵交換処理に成功したとしても、シンク機器3の数を記録するカウンターにより、一時にコンテンツを配布するシンク機器3の数を制限する機能がある。例えば複数のシンク機器3がCopy One Generationでコンテンツを要求したとしても、一定台数のみにCopy One Generationで配布し、一定台数を超えた機器に関しては、認証を受け付けないか、Copy NeverやNo More Copiesで送信し、シンク機器3の数を一定量に制限する。

## 【 0 0 4 7 】

これにより、DTCPネットワークIDを持たない無線基地局2を用いて無線通信システムを構築したとしても、ソース機器1はシンク機器3に対して一定の制限をかけた上でコンテンツを送信することができる。すなわち、ソース機器1から無制限にコンテンツがシンク機器3に対してコピーをすることを防ぐことができる。

。

【 0 0 4 8 】

図 1 0 は無線基地局 2 が DTCP ネットワーク ID を持たない場合の本実施形態の無線通信システムの処理手順を示す図であり、DTCP ネットワーク ID を持たない無線基地局 2 を用いて、シンク機器 3 がソース機器 1 から CCI が No More Copies でコンテンツを受信する手順を示す。

【 0 0 4 9 】

ここでは、無線基地局 2 の DTCP ネットワーク ID が一致しなくとも、シンク機器 3 から CCI が No More Copies でコンテンツを要求される場合に限り、ソース機器 1 はコンテンツを送信できるものとする。

【 0 0 5 0 】

シンク機器 3 はまず無線基地局 2 に対して DTCP ネットワーク ID 認証を試みる（ステップ S 5 1）。無線基地局 2 は DTCP ネットワーク ID を持たないため、この認証処理は失敗する（ステップ S 5 2）。

【 0 0 5 1 】

次に、シンク機器 3 はソース機器 1 に対して CCI が No More Copies で DTCP 認証・鍵交換要求を送る（ステップ S 5 3）。ソース機器 1 はシンク機器 3 からこの DTCP 認証・鍵交換要求を受けると、無線基地局 2 に対して DTCP ネットワーク ID 認証（ステップ S 5 4）を試みる。

【 0 0 5 2 】

DTCP ネットワーク ID の認証を行わないようにしてもよい。認証は失敗する（ステップ S 5 5）が、CCI は No More Copies であるため、ソース機器 1 はシンク機器 3 に対して DTCP 認証・鍵交換処理を行う（ステップ S 5 6）。この認証処理が成功すれば、ソース機器 1 はコンテンツを暗号化してシンク機器 3 に送信する（ステップ S 5 7）。

【 0 0 5 3 】

以上は、無線基地局 2 が DTCP ネットワーク ID を持たない無線基地局の例を示したが、無線基地局 2 とシンク機器 3 の DTCP ネットワーク ID が異なる場合も、同様の処理を行うことでソース機器 1 がシンク機器 3 にコンテンツ送信を制限したり

、拒否することができる。

【 0 0 5 4 】

また、シンク機器 3 とソース機器 1 が無線基地局 2 または、相互の DTCP ネットワーク ID 認証を正常に終了し、DTCP 認証・鍵交換処理が正常に行われたとしても、DTCP 認証・鍵交換処理や DTCP 暗号化コンテンツ送信処理の間に、DTCP ネットワーク ID 認証を行ってもよい。これは、無線基地局 2 が通信中に別の基地局経由に変更されるローミングの攻撃に対してきわめて有効である。

【 0 0 5 5 】

図 1 1 はローミング対策を施した無線通信システムの処理手順を示す図である。図 1 1 に示すように、シンク機器 3 と無線基地局 2 は同一の DTCP ネットワーク IDXX を共有し、ソース機器 1 と無線基地局 2 が同一の DTCP ネットワーク IDYY を共有しているものとする。

【 0 0 5 6 】

ここで、まずシンク機器 3 は、無線基地局 XX に対して DTCP ネットワーク ID 認証を行う（ステップ S 6 1）。無線基地局 XX は同一の値 XX の DTCP ネットワーク ID を持つため、この認証は成功する。この時、シンク機器 3 が無線基地局 XX から無線基地局 YY に基地局を変更したとする。この変更は無線データリンクレイヤーで行われるため、ソース機器 1 やシンク機器 3 内の IEEE802.11 処理部より上のレイヤーはこの変更を知ることができない。

【 0 0 5 7 】

次に、シンク機器 3 はソース機器 1 に対して DTCP 認証要求を送り（ステップ S 6 2）、ソース機器 1 は無線基地局 YY との間で DTCP ネットワーク ID 認証を行う（ステップ S 6 3）。DTCP ネットワーク ID は同一の値 YY を持つため、この認証は成功する。次に、シンク機器 3 とソース機器 1 との間で DTCP 認証・鍵交換処理を行う（ステップ S 6 4）。

【 0 0 5 8 】

ここで、重要なことは、コンテンツの送受信を行う無線基地局が DTCP ネットワーク ID 認証を行った無線基地局とは異なることである。そこで、コンテンツを送受信する際にも、DTCP ネットワーク ID 認証を行う（ステップ S 6 5）。これによ

り、現在通信している無線基地局が、同一のDTCPネットワークIDを持つ機器であることを確認することができる。

【 0 0 5 9 】

本実施形態では、ソース機器 1 とシンク機器 3 が無線基地局 2 を介して、「同一のネットワーク内に存在する機器間ではコンテンツの送受信処理が正常に稼動する」「異なるネットワーク内に存在する機器間では、コンテンツの送受信処理が正常に稼動しない、もしくはコンテンツの送受信に制限をつける」という状況を実現している。

【 0 0 6 0 】

例えば、同一人物A氏が所有するソース機器 1、シンク機器 3 及び無線基地局 2 に同一のIDを付与することで、自分の所有するソース機器 1 から、無線基地局 2 を介してシンク機器 3 にコンテンツを送信することができる。機器の製造者や販売者が無線基地局に一意のIDを付与し、一般の利用者はこのIDを変更できないため、異なる所有者B氏の所有する無線基地局 5 のIDはA氏の保有する無線基地局 2 のIDとは異なる。従って、B氏の保有するシンク機器やソース機器 4 はB氏の保有する無線基地局 5 のIDに設定されており、B氏のソース機器からA氏のシンク機器 3 にコンテンツが送信されない、という環境を実現できる。

【 0 0 6 1 】

つまり、一般的にインターフェースが無線の場合、シンク機器 3、無線基地局 2 及びソース機器 1 が電波の受信範囲内にあれば、シンク機器 3 は異なるIDの付与されたソース機器 1 に対してコンテンツ要求の指示を送信できる。したがって、ソース機器 1 と無線基地局 2 の所有者M氏の無線基地局のIDを知りえるN氏は自分のシンク機器のIDをM氏の無線基地局のIDに設定することで、ソース機器に蓄積されたM氏のコンテンツが受信可能となり、M氏は悪意の有無に限らずコンテンツを自由に配布する環境を構築できてしまう。

【 0 0 6 2 】

同様の理由から、O氏の保有する無線基地局のIDを知りえるP氏とQ氏は、自己のソース機器やシンク機器のIDをO氏の無線基地局のIDに設定することで、O氏の意図に限らず、またO氏はP氏やQ氏の意図を知ることなくコンテンツを送受信で

きてしまう。

【 0 0 6 3 】

そこで、本実施形態では、シンク機器 3 とソース機器 1 の ID の変更回数を制限することで、シンク機器 3 やソース機器 1 の所属するネットワークの変更を制限している。

【 0 0 6 4 】

さて、図 1 において、シンク機器 3 がローカルエリア無線ネットワーク A からローカルエリア無線ネットワーク B に移動した時など、ローカルエリア無線ネットワークの DTCP ネットワーク ID が変化した場合には、シンク機器 3 とソース機器 1 の DTCP ネットワーク ID を無線基地局 2 に対応した ID から無線基地局 5 に対応した ID に変更すればよい。

【 0 0 6 5 】

また、無線基地局 2 の DTCP ネットワーク ID 記録部 1 3 に記録されている DTCP ネットワーク ID は、機器の製造者または販売者等に、買い替え前の無線基地局の DTCP ネットワーク ID を申請することで、DTCP ネットワーク ID が同一の無線基地局を購入できるようにしてもよい。

【 0 0 6 6 】

上述した説明では、ソース機器 1 とシンク機器 3 が同一の DTCP ネットワーク ID を持つ一つの無線基地局 2 を介してコンテンツを送受信する場合を考えてきた。ところが、同一の所有者 A 氏が 2 つ以上の無線基地局を所有する場合も考えられる。この場合、複数の無線基地局、ソース機器 1 及びシンク機器 3 の DTCP ネットワークを接続するには種々の方法がある。例えば、（１）DTCP ネットワーク ID を指定して無線基地局を購入する方法、（２）DTCP ネットワーク ID を記録するレジスタを複数用意する方法などがある。

【 0 0 6 7 】

また、悪意のあるソース機器 1 の保有者が、ソース機器 1 と無線基地局 2 の DTCP ネットワーク ID を公開し、著作権者の許可なしにコンテンツを配布できる環境を構築していることが発覚した場合、当該ソース機器 1 または無線基地局 2 の DTCP ネットワーク ID を無効にするリボケーションの仕組みがあれば、著作権者にとっ

て有益である。

【 0 0 6 8 】

図 1 2 はリボケーション機能をもつソース機器 1 の内部構成を示すブロック図である。図 1 2 の無線通信システムは、図 3 の構成に、無効な DTCP ネットワーク ID のリストを保存する不正機器リスト記録部 3 0 を追加したものである。一般の利用者は、不正機器リスト記録部 3 0 の内容を書き換えることはできない。

【 0 0 6 9 】

図 1 3 は図 1 2 のソース機器の処理手順を示す図である。図 8 の処理と異なり、無線基地局 1 との間で DTCP ネットワーク ID 認証処理を行う前に、無線基地局 1 のネットワーク ID が不正機器リスト記録部 3 0 に記録されているか否かを判定し（ステップ S 3 7）、記録されている場合には、不正機器と判断してエラー処理を行う（ステップ S 3 8）。

【 0 0 7 0 】

なお、不正機器リスト記録部を無線基地局の内部に設けてもよい。この場合、無線基地局は、ネットワーク ID 認証を行う前に、不正機器リスト記録部をチェックし、同記録部に記録されている送信装置との間ではネットワーク ID 認証を行わないようにする。

【 0 0 7 1 】

このように、第 1 の実施形態では、DTCP ネットワーク ID の変更回数を制限するようにしたため、著作権保護を図る必要のあるコンテンツの悪用を防止できる。また、認証に失敗した場合に、コンテンツの送信を完全に禁止するのではなく、一定の制限をかけた上でコンテンツの送信を認めるようにしたため、著作権保護を図りつつ、ユーザの使い勝手を向上できる。

【 0 0 7 2 】

さらに、ローミング対策として、所定時間ごとに DTCP ネットワーク ID の認証を繰り返すようにしたため、ローミングによるコンテンツの悪用を防止できる。

【 0 0 7 3 】

また、無効な DTCP ネットワーク ID のリストを保存しておくことにより、不正機器を迅速に発見できる。



【 0 0 7 4 】

(第 2 の実施形態)

上述した第 1 の実施形態では、ソース機器 1 が無線基地局 2 を介してシンク機器 3 にコンテンツを送信していた。これに対して、第 2 の実施形態は、無線基地局を介さずに、ソース機器 1 がシンク機器 3 に対して直接コンテンツを送信するものである。

【 0 0 7 5 】

IEEE802.11では、無線基地局を介さずに無線機器が通信するアドホックモードと呼ばれる通信形態が規定されている。本実施形態はアドホックモードを利用して通信を行うものであり、以下では、第一の実施形態と相違する部分を中心に説明する。

【 0 0 7 6 】

図 1 4 は本発明に係る無線通信システムの第 2 の実施形態の概略構成を示すブロック図である。図 1 4 に示すように、ソース機器 1 とシンク機器 3 a, 3 b, 3 c は、互いに通信可能な範囲内にあり、各シンク機器 3 a, 3 b, 3 c は X 氏の所有物であるとする。ソース機器 1 は、各シンク機器 3 a, 3 b, 3 c と DTCP ネットワーク ID 認証を行うために、各シンク機器 3 a, 3 b, 3 c の DTCP ネットワーク ID をネットワーク ID 記録部に記録している。

【 0 0 7 7 】

第 1 の実施形態では、所有者が自由に変更できない DTCP ネットワーク ID が予め無線基地局 2 に設定されており、ソース機器 1 とシンク機器 3 の DTCP ネットワーク ID を無線基地局 2 の値と同一に設定することで、無線基地局 2 を介したコンテンツの送受信を行っていた。これに対して、第 2 の実施形態では、無線基地局が存在しないため、ソース機器 1 とシンク機器 3 a, 3 b, 3 c は DTCP ネットワーク ID に任意の値を設定する。

【 0 0 7 8 】

しかしながら、ソース機器 1 やシンク機器 3 a, 3 b, 3 c が記録可能な DTCP ネットワーク ID の数は DTCP ネットワーク ID 記録部によって一定数に制限されている。また、ソース機器 1 とシンク機器 3 a, 3 b, 3 c は同一の DTCP ネットワー

クIDを記録しておかなければならないため、DTCPネットワークIDを変更しない限り、ソース機器1は一定数以上のシンク機器にはコンテンツを送信できない。同様の理由から、シンク機器は一定数以上のソース機器からコンテンツを受信できない。

【0079】

この問題を解決する方法として、X氏の所有するすべての機器のDTCPネットワークIDを統一させてしまう方法がある。

【0080】

ところが、図15に示すように、すべての機器のDTCPネットワークIDを同じにしてしまうと、無線機器の所有者に関わらず、すべての機器間のDTCPネットワークID認証が成功してしまう。これでは、悪意のあるシンク保有者によるコンテンツ配布を防止できない。

【0081】

このため、アドホックモードで通信する場合は、インフラストラクチャモードのDTCPネットワークID認証が失敗したときと同じエラー処理を行い、制限をかけた上でコンテンツを送信するようにすればよい。

【0082】

すなわち、(1)シンク機器から受信したDTCP認証要求を破棄し、DTCP認証処理を終了させる方法、(2)コピー制限のレベルを変更する方法、(3)コンテンツを配布するシンク機器の台数を制限する方法、(4)上記の(2)と(3)をの全部又は一部を併用する方法など種々の方法が考えられる。

【0083】

図16は無線通信システムのアドホックモードにおける処理手順を示す図である。まず、シンク機器3a, 3b, 3cはソース機器1に対してDTCP認証要求を行う(ステップS71)。この要求を受けて、ソース機器1は、制限をかけた通信を許可する(ステップS72)。次に、ソース機器1とシンク機器3a, 3b, 3cとの間でDTCP認証・鍵交換処理を行う(ステップS73)。次に、交換した鍵を用いて暗号化したコンテンツをソース機器1からシンク機器3a, 3b, 3cに送信する(ステップS74)。

## 【 0 0 8 4 】

図 1 7 はシンク機器 3 a, 3 b, 3 c の処理手順を示す図である。シンク機器 3 a, 3 b, 3 c は通信に先立ち、ソース機器 1 との通信形態を確認する（ステップ S 8 1）。通信形態がアドホックモードの場合、DTCP ネットワーク ID 認証を行なわない。もちろん、DTCP ネットワーク ID 認証処理を行なっても良いが、認証の成否に関わらず、ソース機器 1 に DTCP 認証要求を送信する（ステップ S 8 2）。

## 【 0 0 8 5 】

一方、通信形態がインフラストラクチャモードの場合、無線基地局との間で DTCP ネットワーク ID の認証処理を行う（ステップ S 8 3）。

## 【 0 0 8 6 】

次に、DTCP ネットワーク ID が一致するか否かを判定し（ステップ S 8 4）、一致しなければステップ S 8 2 の処理を行い、一致するとソース機器 1 との間で認証・鍵交換処理を行う（ステップ S 8 5）。

## 【 0 0 8 7 】

図 1 8 はソース機器 1 の処理手順を示す図である。ソース機器 1 は、シンク機器 3 a, 3 b, 3 c からの DTCP 認証処理要求を受けると（ステップ S 9 1）、次に、通信形態を確認する（ステップ S 9 2）。

## 【 0 0 8 8 】

通信形態がアドホックモードの場合、シンク機器 3 a, 3 b, 3 c の要求がソース機器 1 の制限を満たしていれば、DTCP 認証を受け付ける（ステップ S 9 3）。例えば、ソース機器 1 が接続するシンク機器の台数を 1 台に制限していた場合、二台目以降に接続したシンク機器の要求は拒否される。

## 【 0 0 8 9 】

一方、シンク機器が No More Copies を 5 台まで許可するように制限していた場合、2 台目に接続したシンク機器が No More Copies で DTCP 認証を要求していれば、この要求は受け付けられる。

## 【 0 0 9 0 】

一方、通信形態がインフラストラクチャモードの場合、基地局との間で DTCP ネットワーク ID の認証処理を行う（ステップ S 9 4）。

ットワークID認証処理を行い（ステップS 9 4）、DTCPネットワークIDが同一か否かを判定する（ステップS 9 5）。同一でなければステップS 9 3の処理を行い、同一であれば認証・鍵交換処理を行う（ステップS 9 6）。

【 0 0 9 1 】

第2の実施形態は、第1の実施形態に比べ、通信形態がアドホックモードのみをサポートするソース機器1やシンク機器3 a, 3 b, 3 cであれば、DTCPネットワークID認証処理は必ずしも必要ではないため、装置構成を単純化することができる。

【 0 0 9 2 】

例えば、X氏が携帯型のシンク機器（例えばディスプレイ装置など）を所有していた場合、X氏はY氏のソース機器（例えばDVD再生装置など）からのコンテンツの保存を必ずしも要求しておらず、その場限りの閲覧のみを希望している場合には、アドホックモードにより設定をすることなく無線通信システムを構築し、Y氏のソース機器からX氏のシンク機器にコンテンツを送信することが可能となる。

【 0 0 9 3 】

このように、第2の実施形態では、アドホックモードで通信を行う場合は、コピーを許可しないようにしてコンテンツを送信するため、各シンク機器が任意にDTCPネットワークIDを設定しても、コンテンツの違法コピーを確実に防止できる。

【 0 0 9 4 】

なお、上述した各実施形態では、無線LANとしてIEEE802.11を例に説明してきたが、本発明はBluetoothなど種々の無線LANに適用することが可能である。

【 0 0 9 5 】

【発明の効果】

以上詳細に説明したように、本発明によれば、認証及び鍵交換を行う受信装置の数を通信モードによって切り替えるため、著作権保護が必要なコンテンツの悪用を防止できる。

【 0 0 9 6 】

また、認証に失敗した場合に、コンテンツの送信を完全に禁止するのではなく、一定の制限をかけた上でコンテンツの送信を認めるようにしたため、著作権保護を図りつつ、ユーザの使い勝手を向上できる。

【図面の簡単な説明】

【図 1】

本発明に係る送信装置、受信装置及び無線基地局を含む無線通信システムの第 1 の実施形態の全体構成を示すブロック図。

【図 2】

無線基地局の内部構成の一例を示すブロック図。

【図 3】

ソース機器の内部構成の一例を示すブロック図。

【図 4】

シンク機器の内部構成の一例を示すブロック図。

【図 5】

本実施形態の無線通信システムの処理手順を示す図。

【図 6】

シンク機器の処理手順を示す図。

【図 7】

図 6 のステップ S 1 8 のエラー処理手順を示す図。

【図 8】

ソース機器の処理手順を示す図。

【図 9】

図 8 のステップ S 3 6 のエラー処理手順を示す図。

【図 1 0】

無線基地局が DTCP ネットワーク ID を持たない場合の本実施形態の無線通信システムの処理手順を示す図。

【図 1 1】

ローミング対策を施した無線通信システムの処理手順を示す図。

【図 1 2】

リボケーション機能をもつソース機器の内部構成を示すブロック図。

【図 1 3】

図 1 2 のソース機器の処理手順を示す図。

【図 1 4】

本発明に係る無線通信システムの第 2 の実施形態の概略構成を示すブロック図

【図 1 5】

すべての機器のDTCPネットワークIDを同じにした例を示す図。

【図 1 6】

無線通信システムのアドホックモードにおける処理手順を示す図。

【図 1 7】

シンク機器の処理手順を示す図。

【図 1 8】

ソース機器 1 の処理手順を示す図。

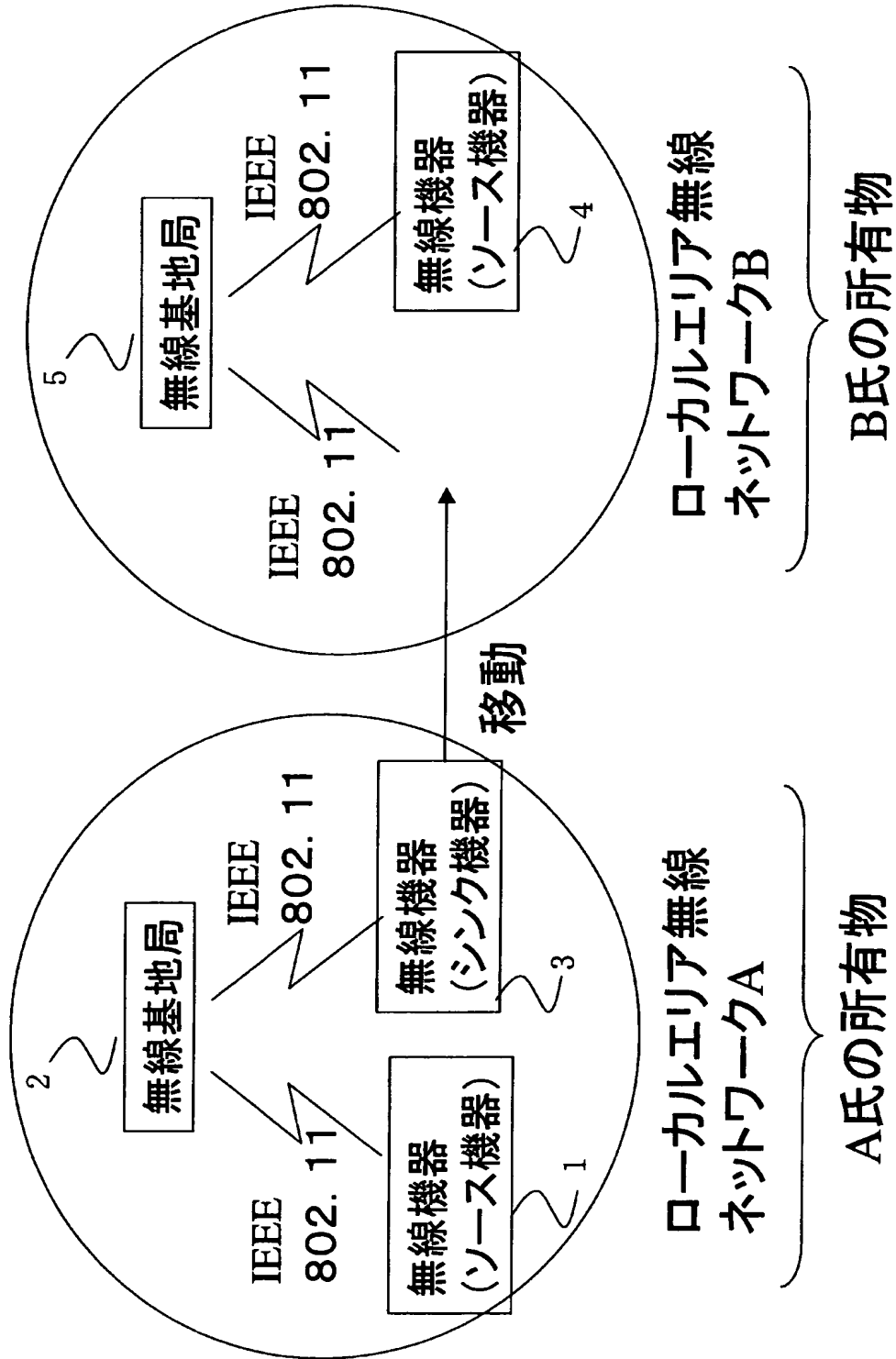
【符号の説明】

- 1, 4 ソース機器
- 2, 5 無線基地局
- 3 シンク機器
- 1 1 802.11インターフェース処理部
- 1 2 通信処理部
- 1 3 DTCPネットワークID記録部
- 2 1 コンテンツ蓄積部
- 2 2 パケット処理部
- 2 3 DTCP認証・鍵交換処理部
- 2 4 DTCP暗号・復号処理部
- 2 5 802.11通信処理部
- 2 6 802.11インターフェース部
- 2 7 DTCPネットワークID入力部
- 2 8 DTCPネットワークID記録部

- 2 9 DTCPネットワークID認証処理部
- 3 1 コンテンツ再生処理部
- 3 2 パケット処理部
- 3 3 DTCP認証・鍵交換処理部
- 3 4 DTCP暗号・復号処理部
- 3 5 802.11通信処理部
- 3 6 802.11インターフェース部
- 3 7 DTCPネットワークID入力部
- 3 8 DTCPネットワークID記録部
- 3 9 DTCPネットワークID認証処理部

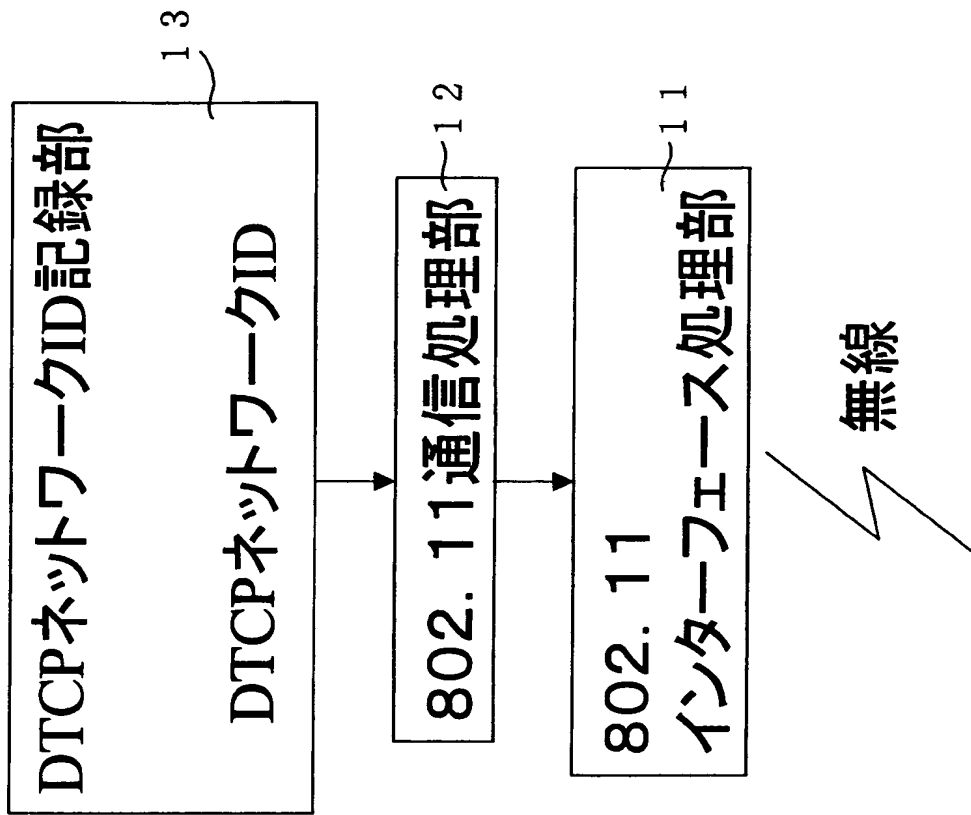
【書類名】 図面

【図 1】

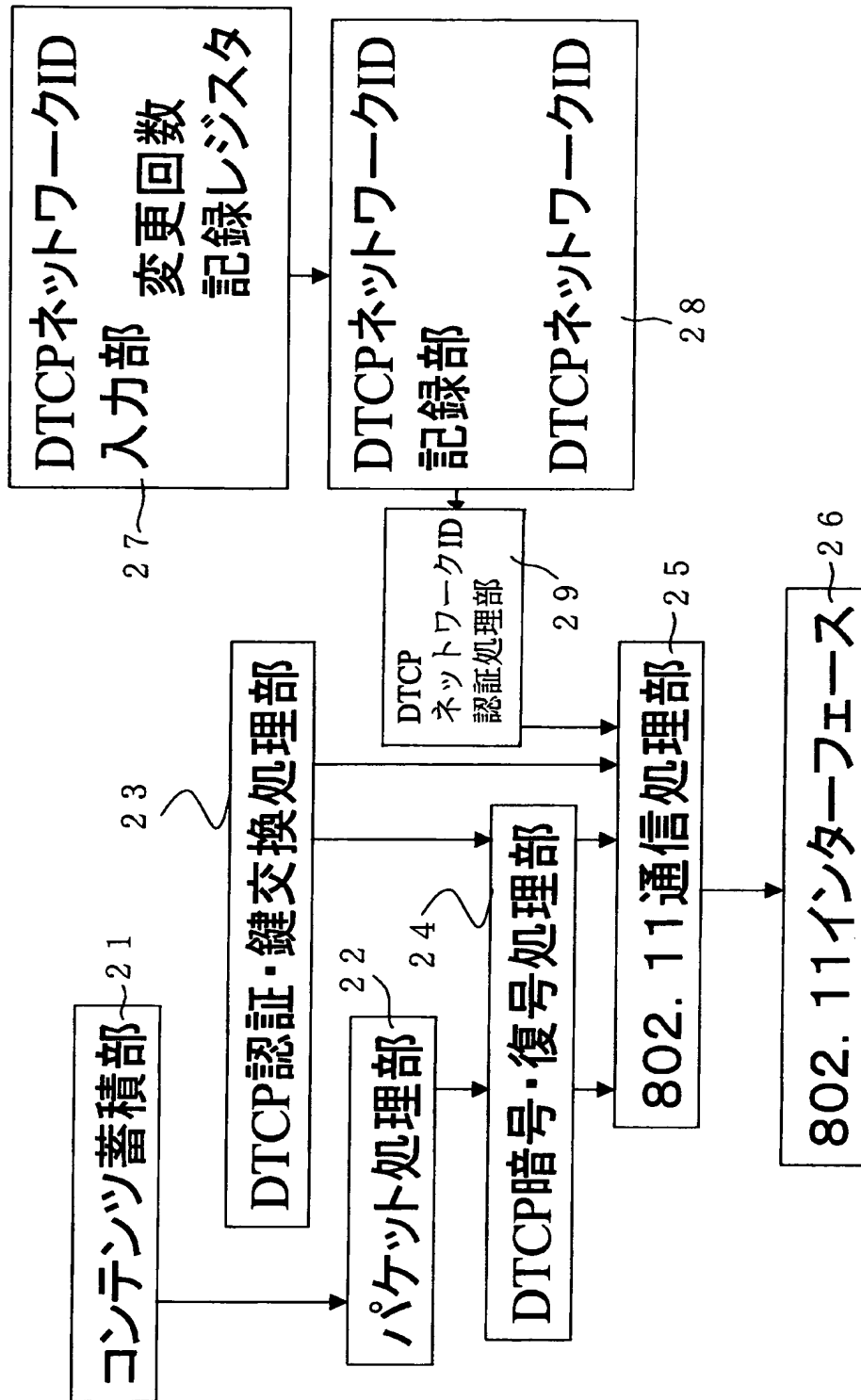




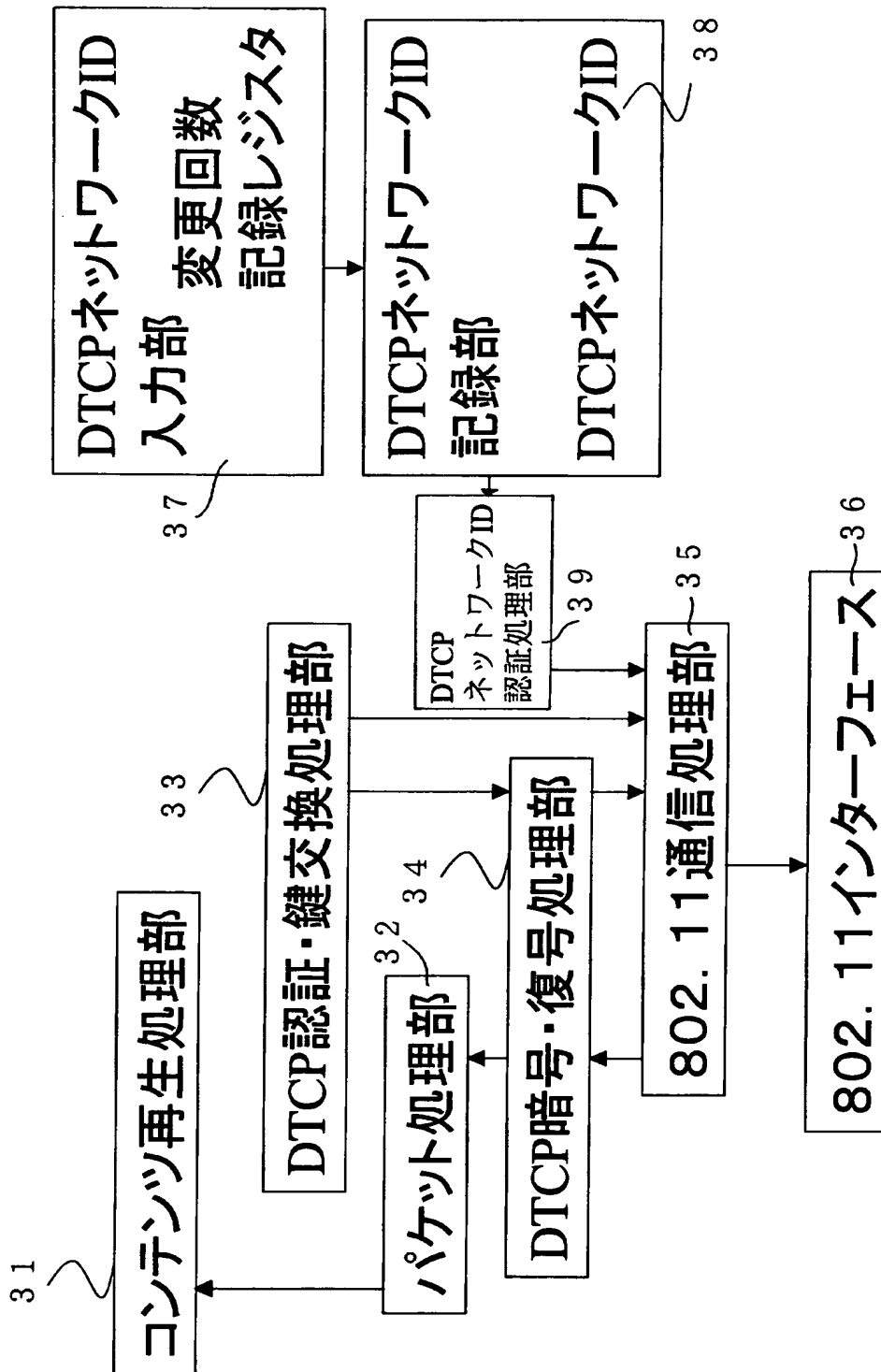
【図 2】



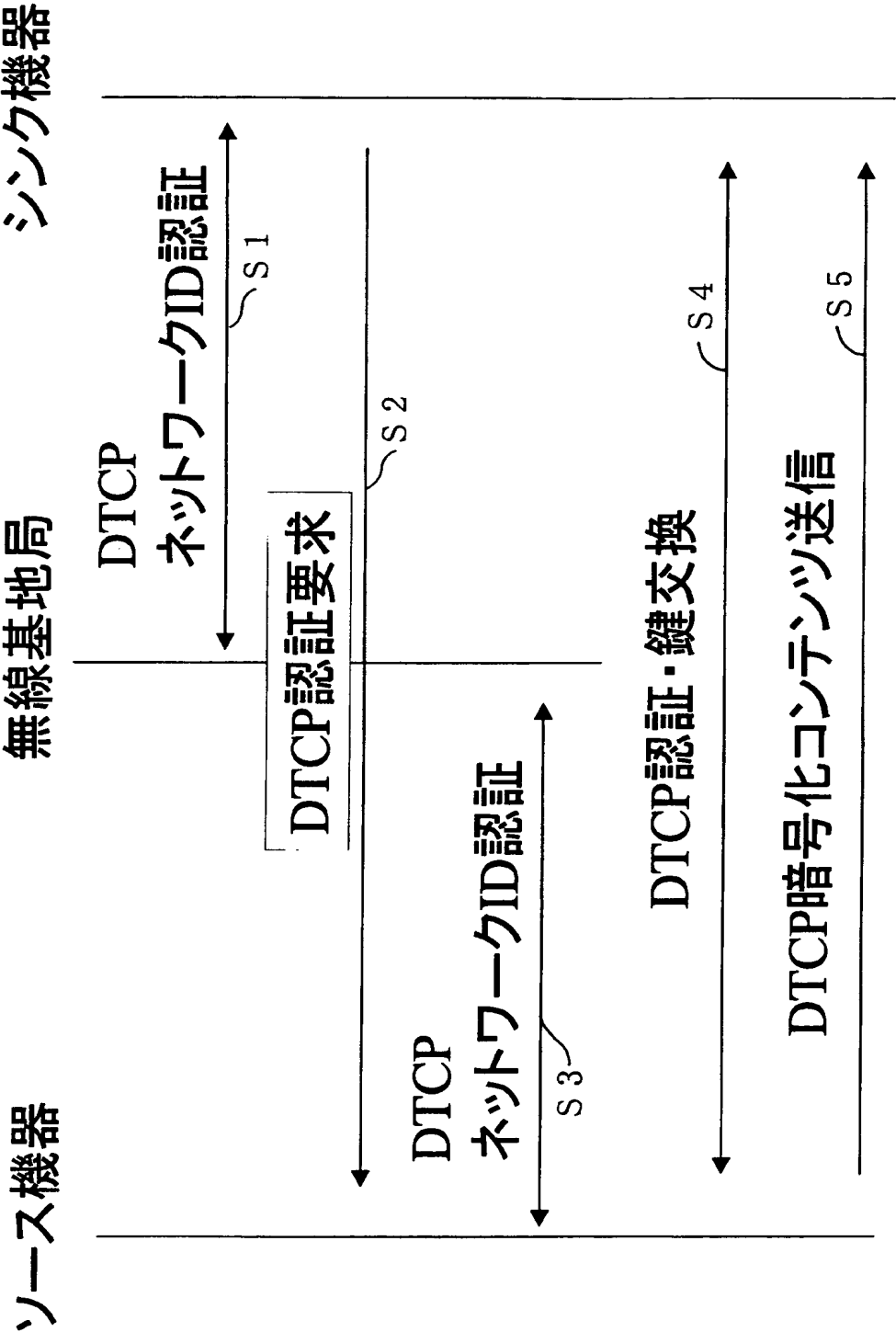
【図 3】



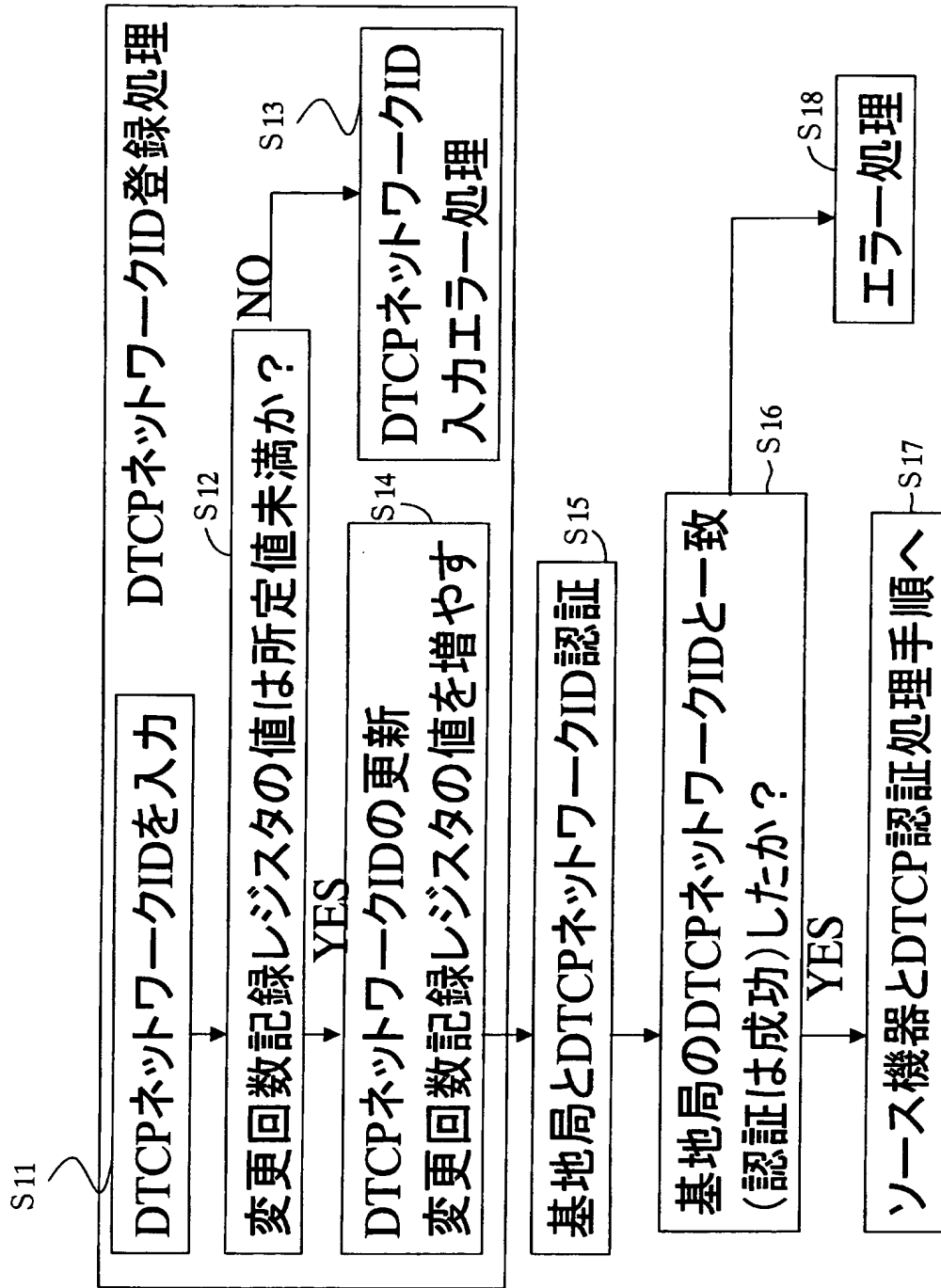
【図 4】



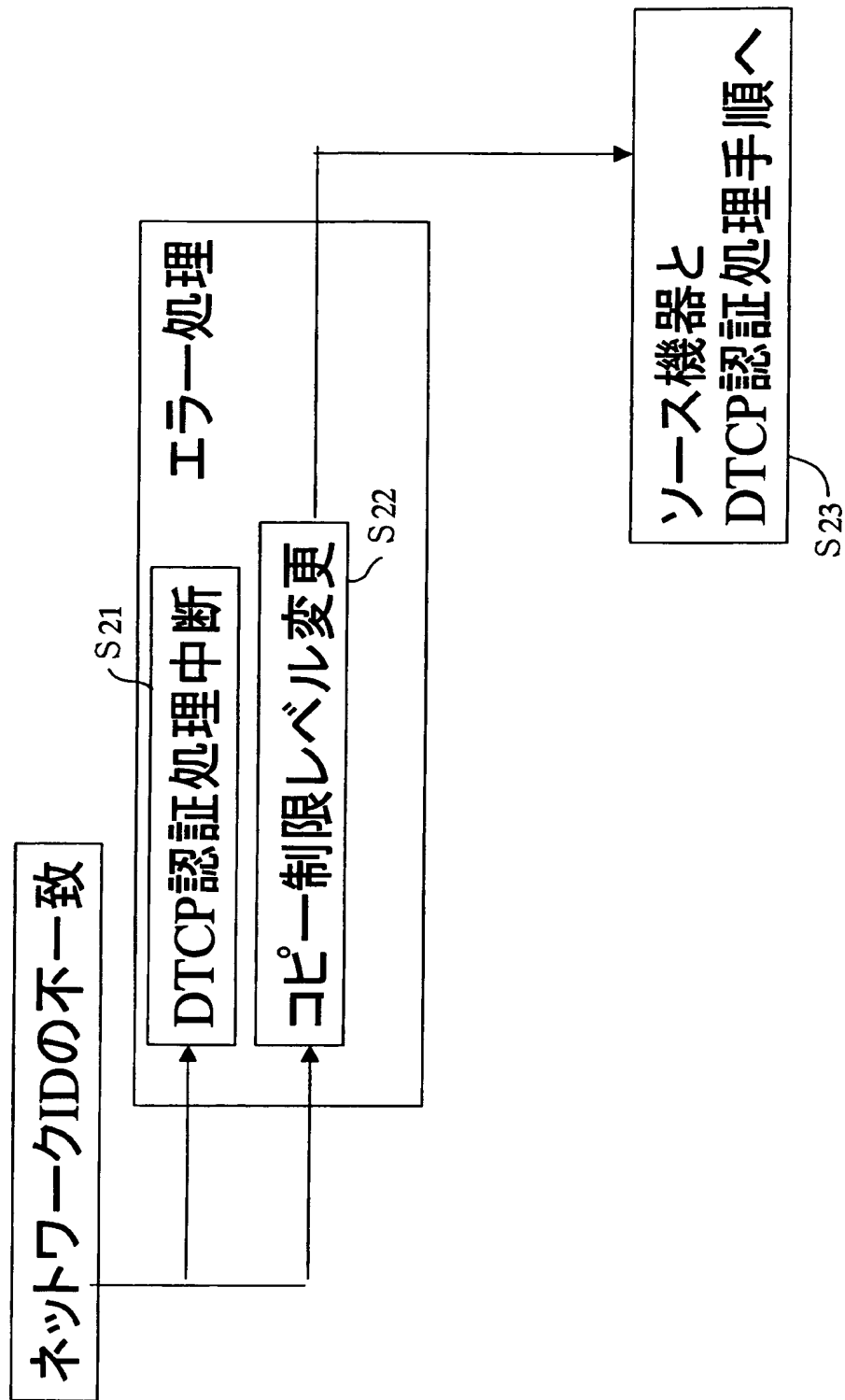
【図 5】



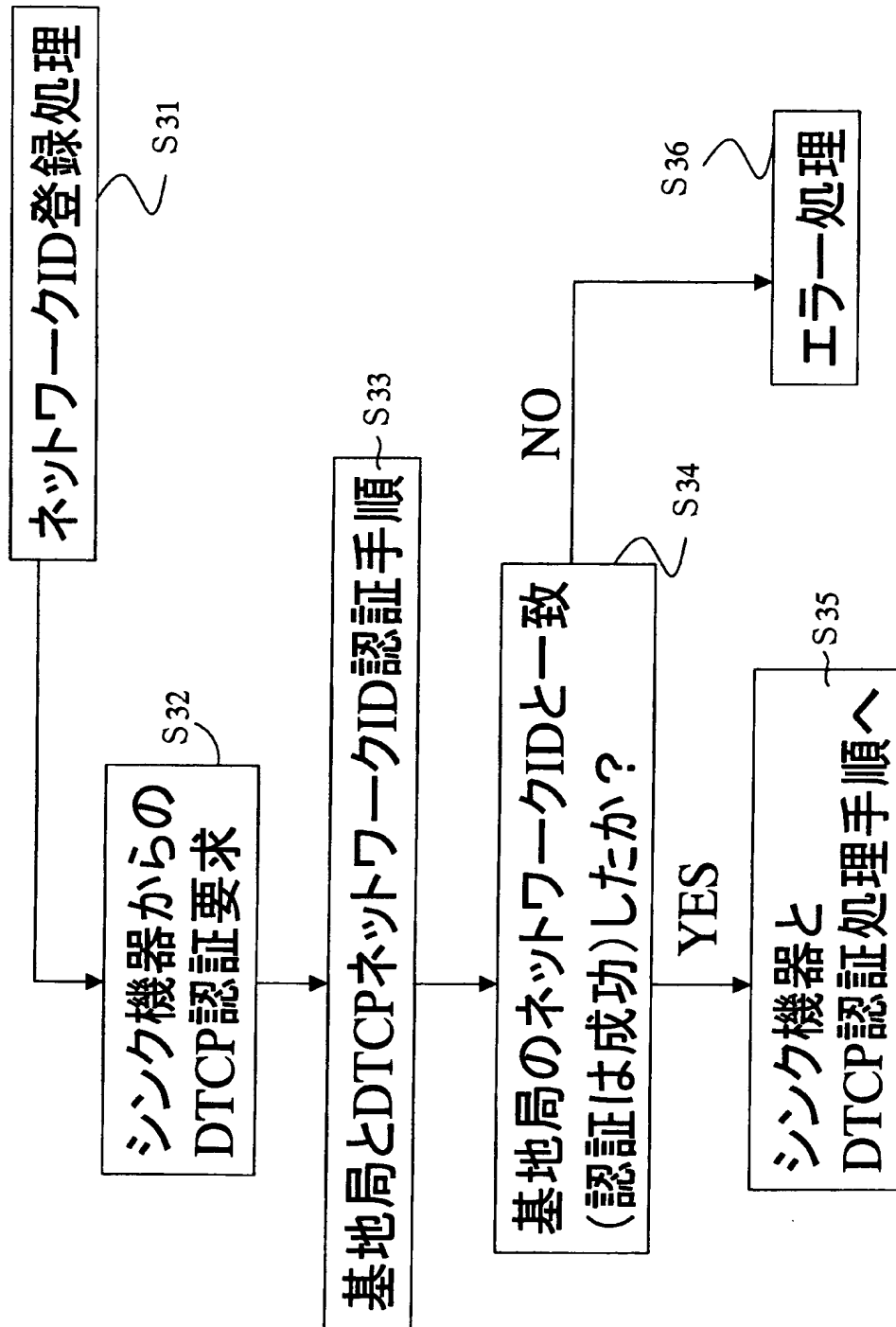
【図 6】



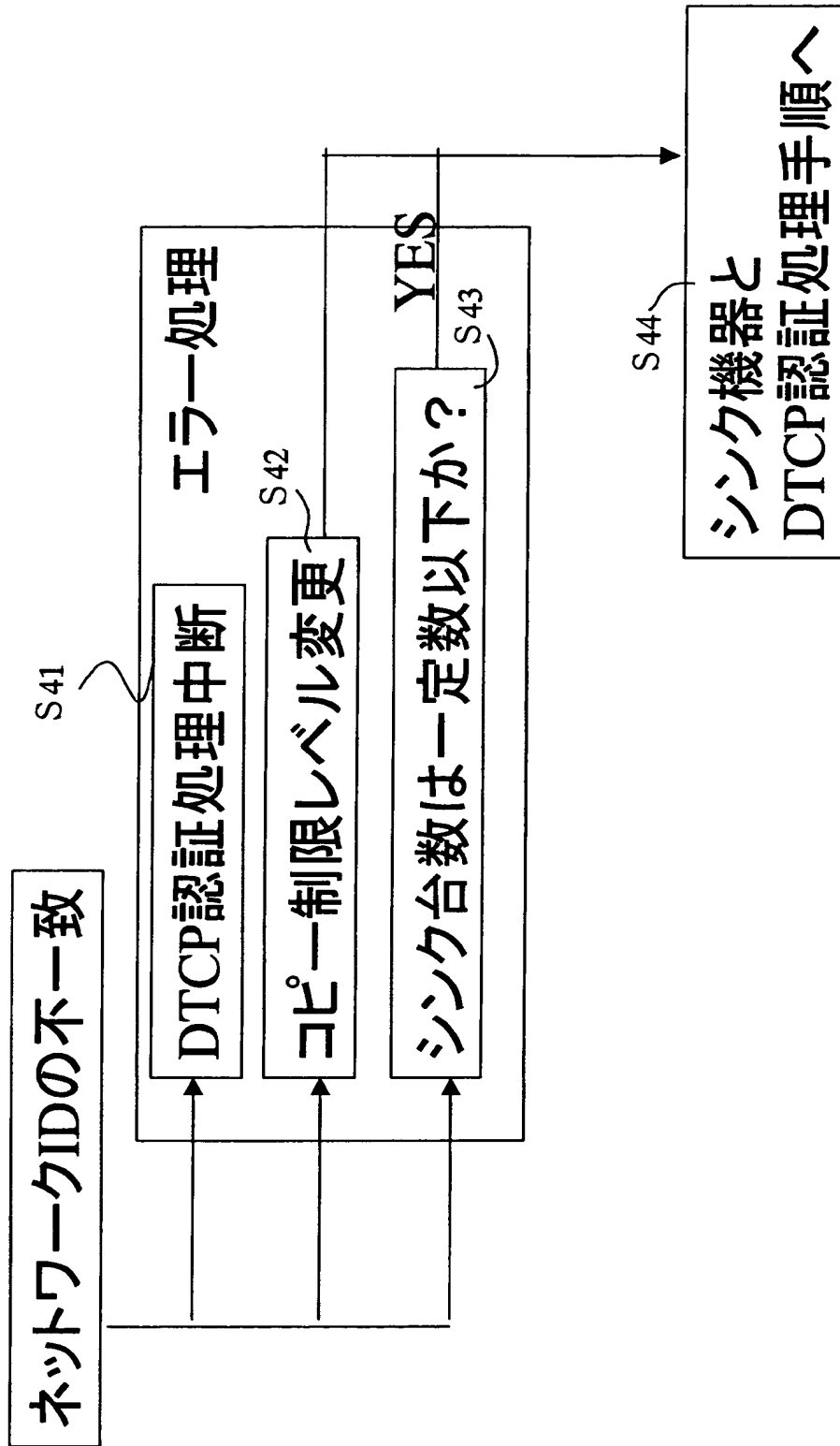
【図 7】



【図 8】

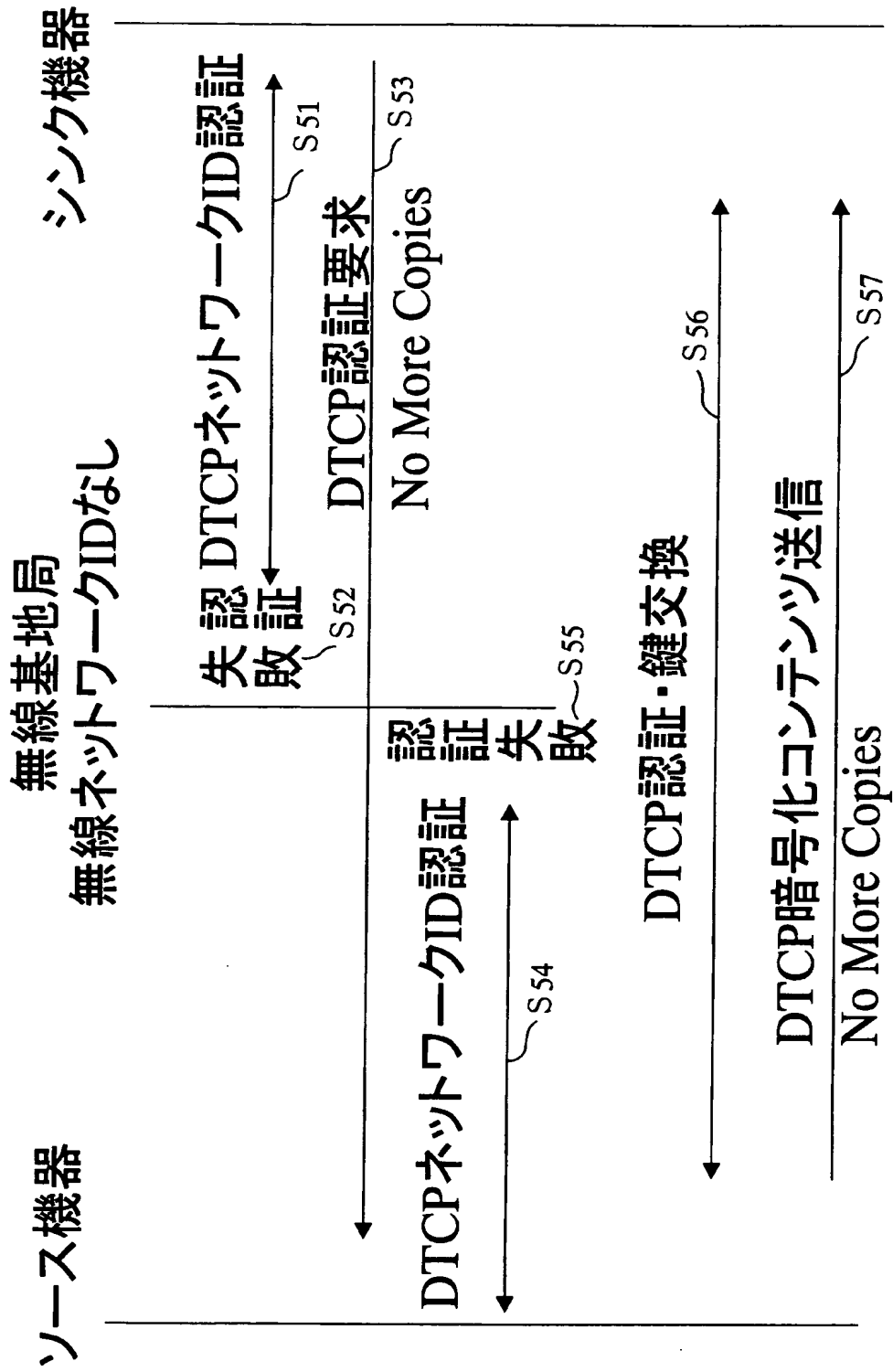


【図 9】

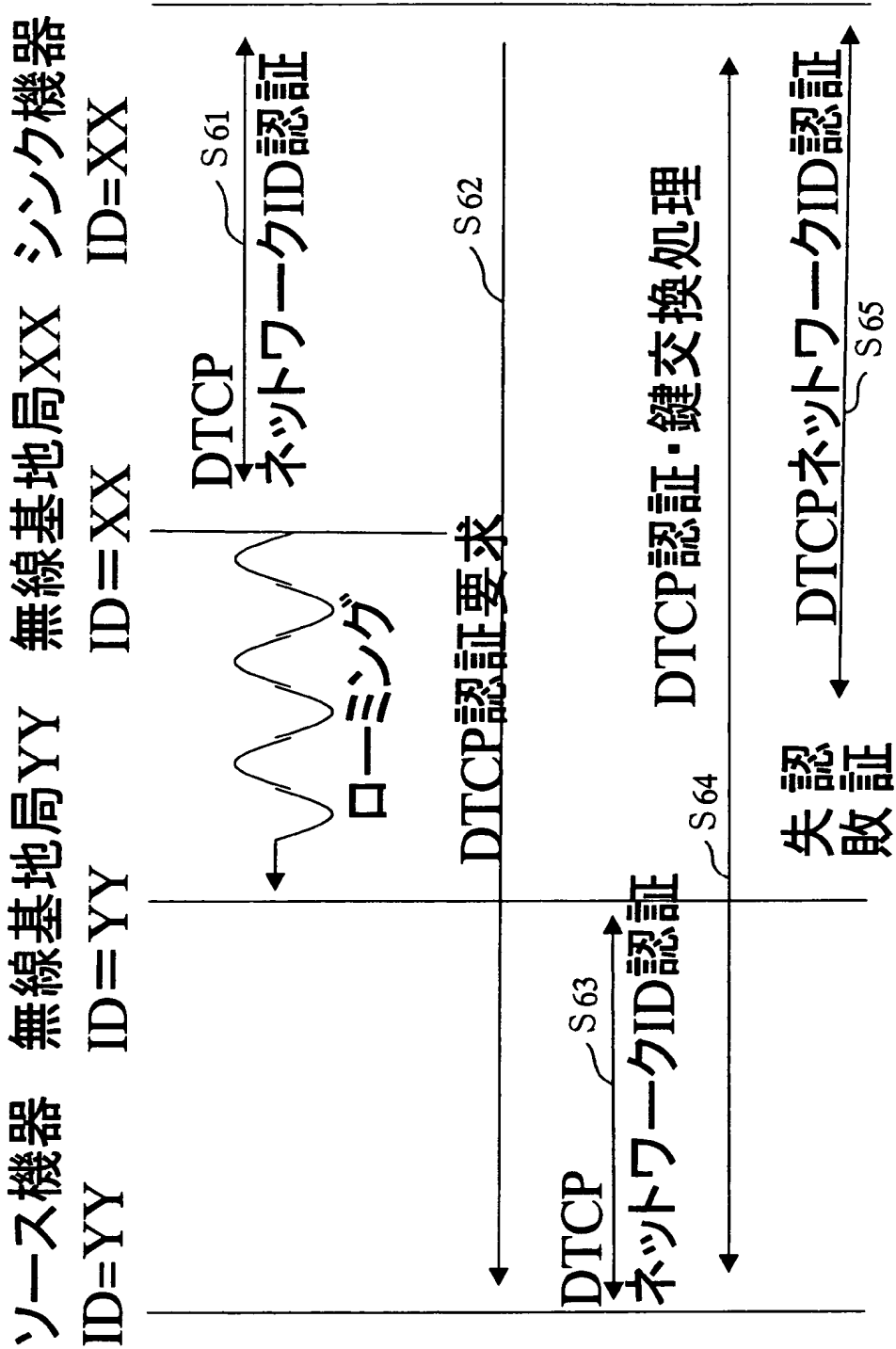




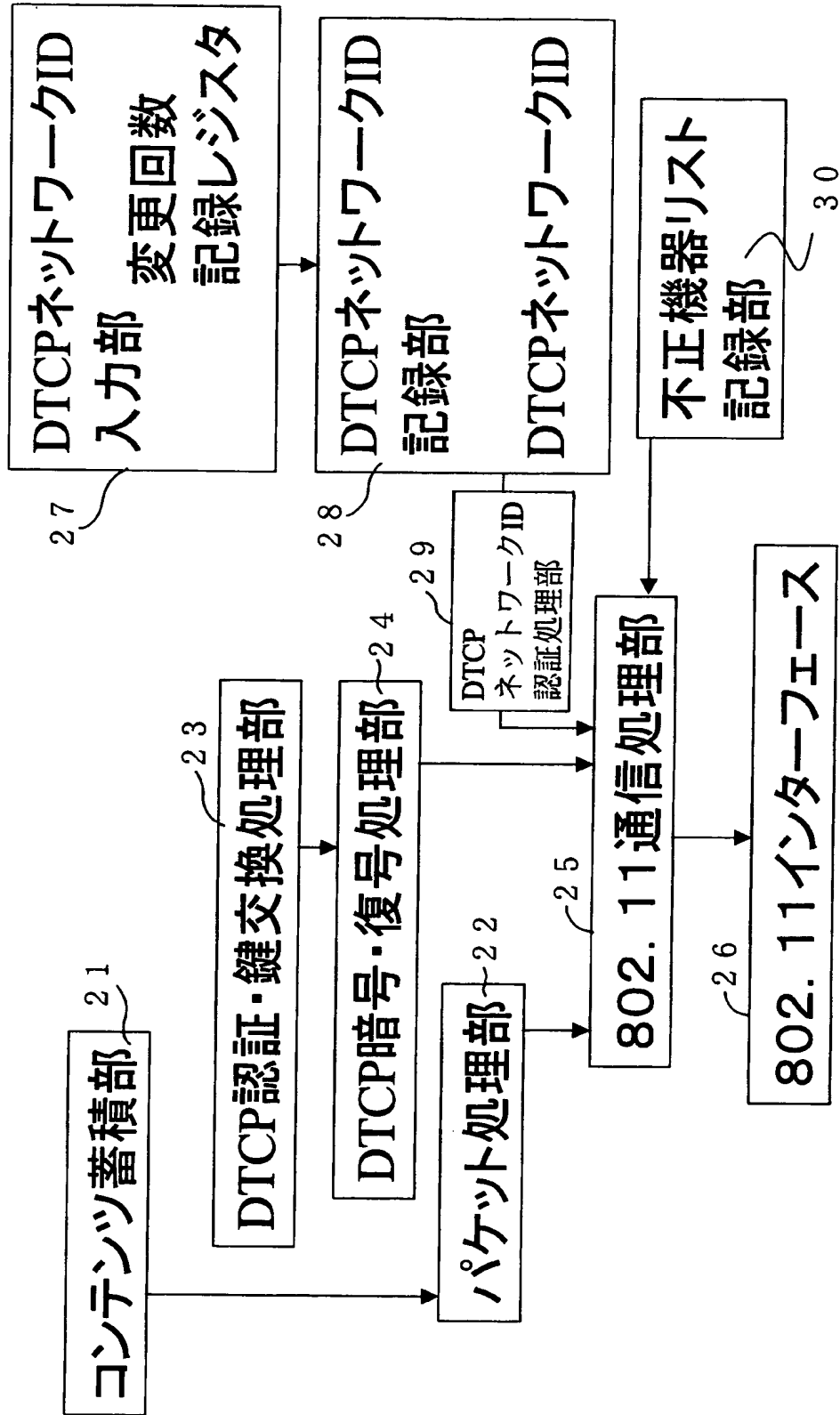
【図 1 0】



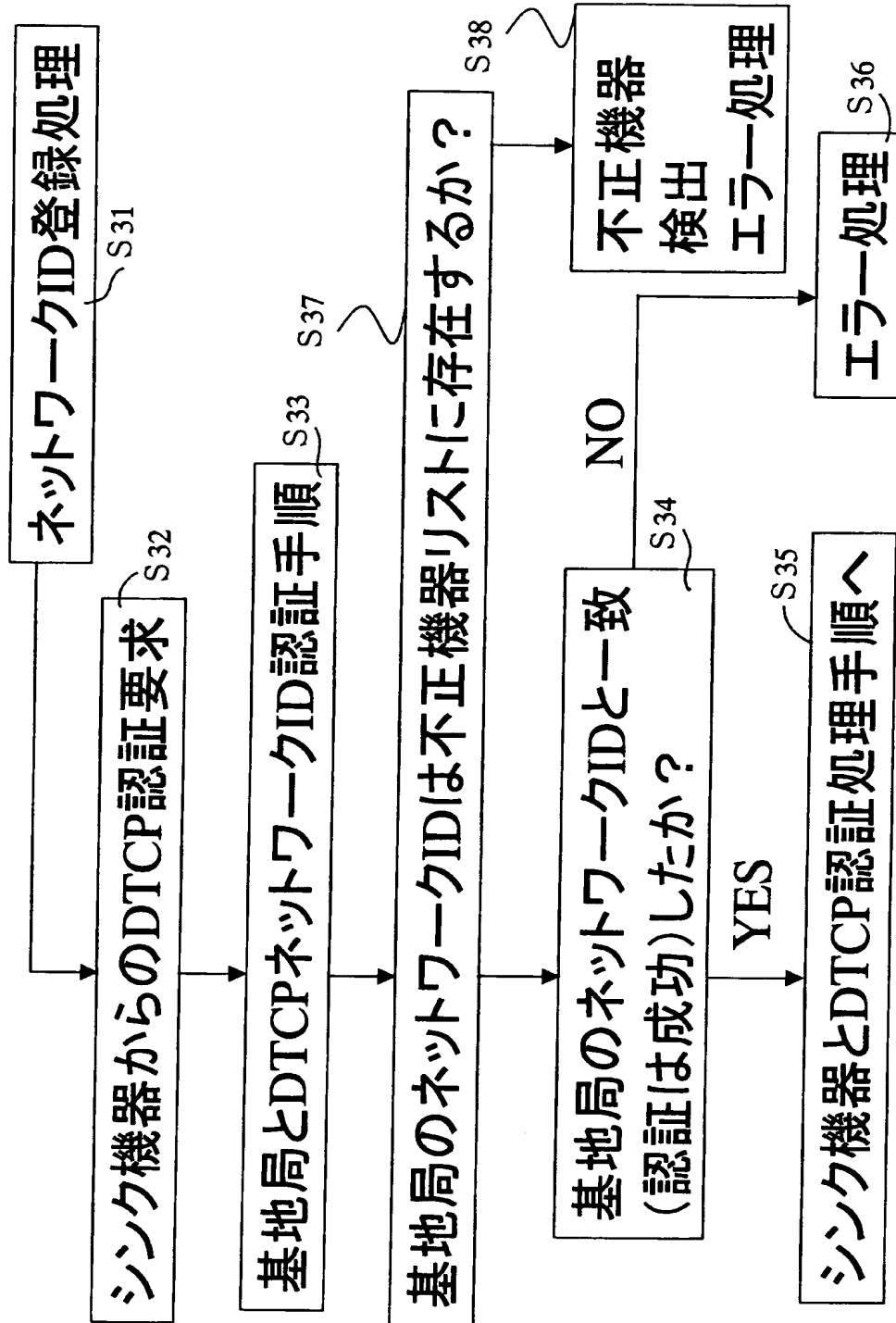
【図 1 1】



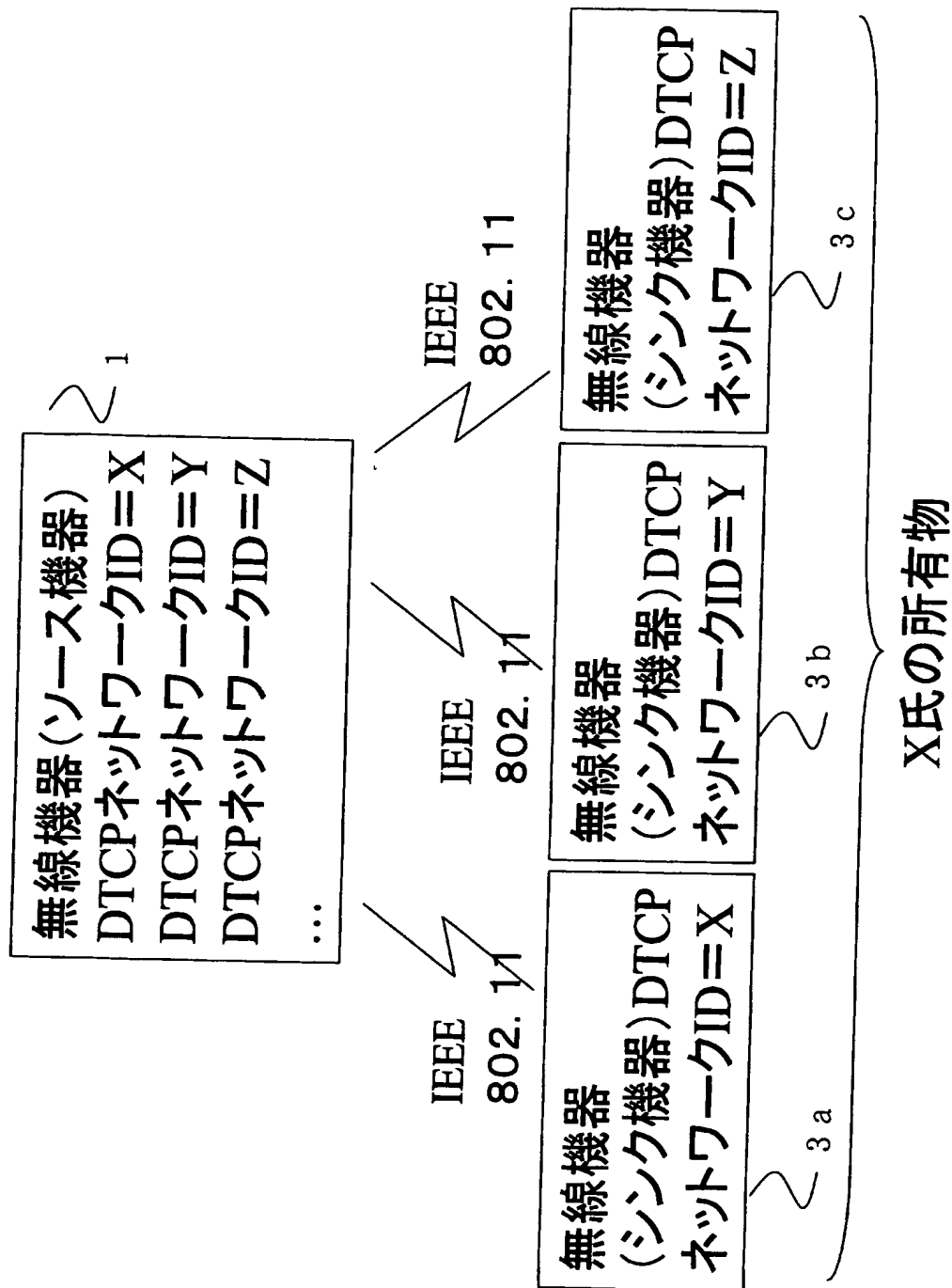
【図 1 2】



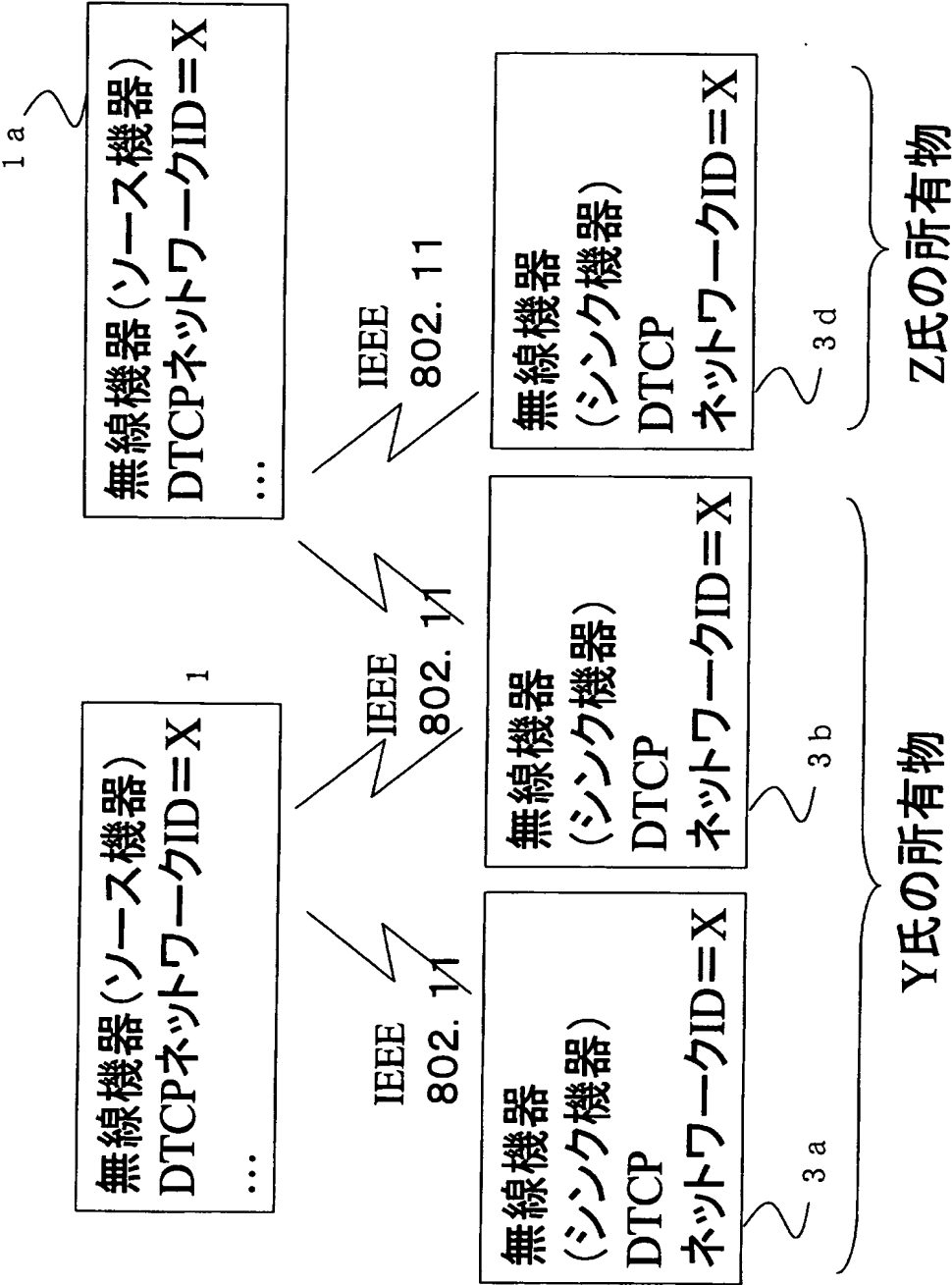
【図 1 3】



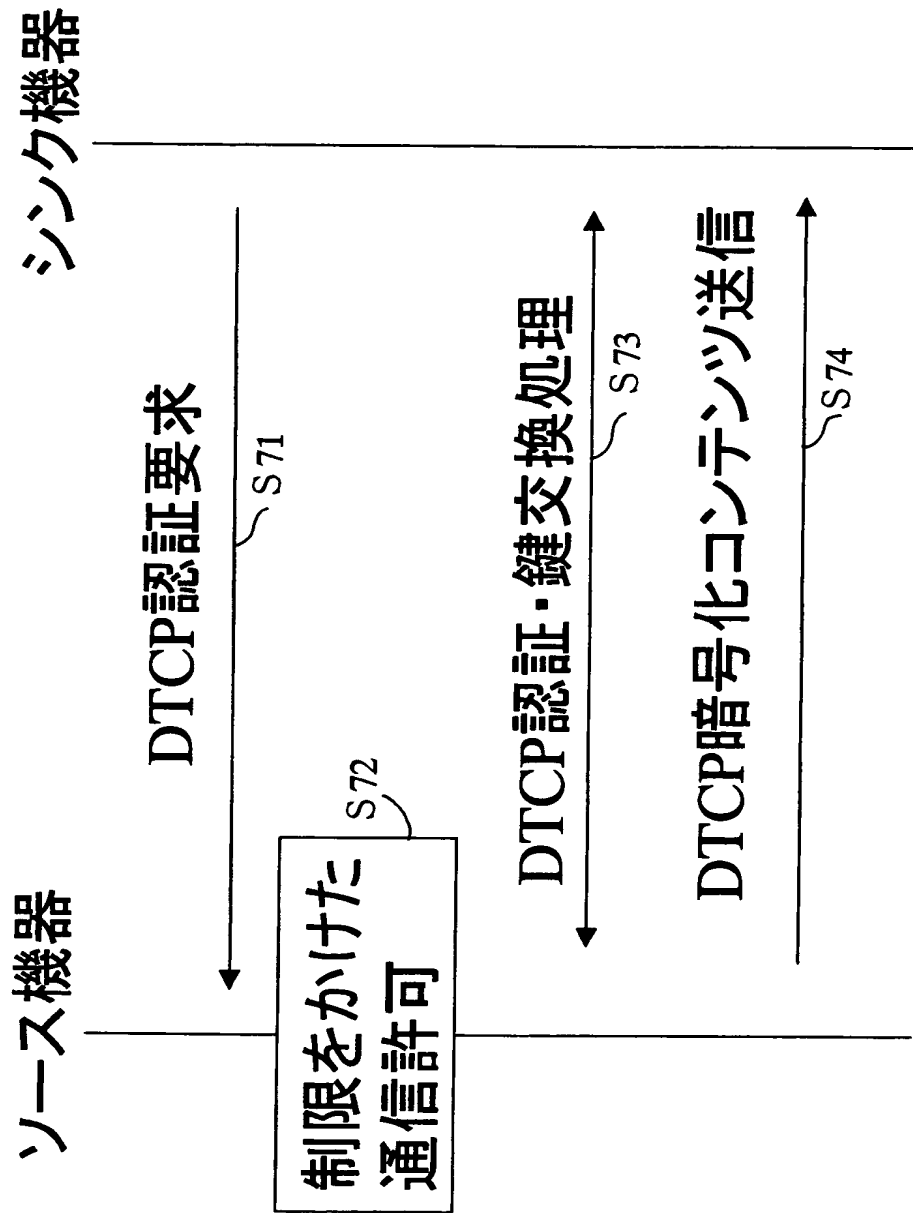
【図 1 4】



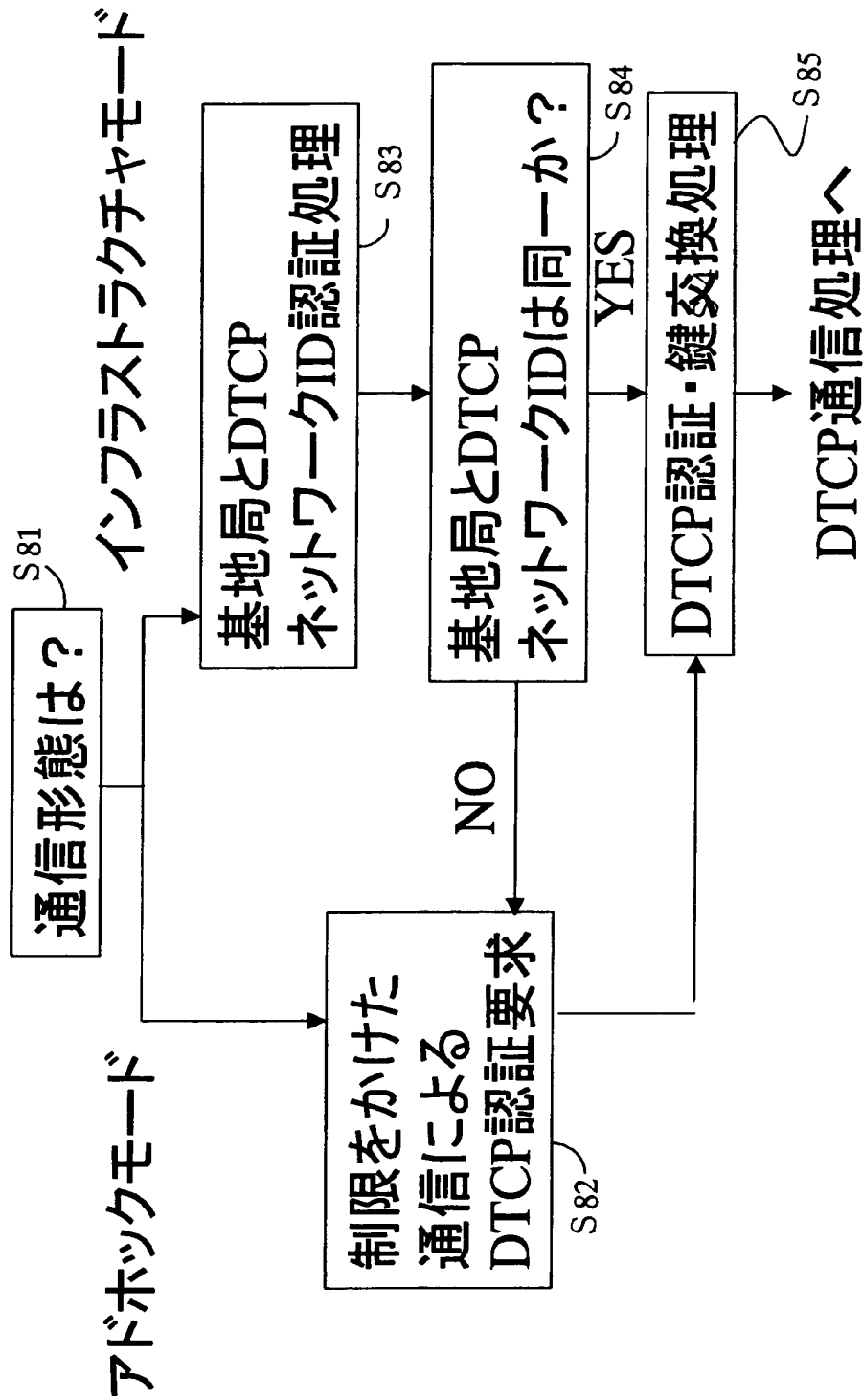
【図 1 5】



【図 1 6】

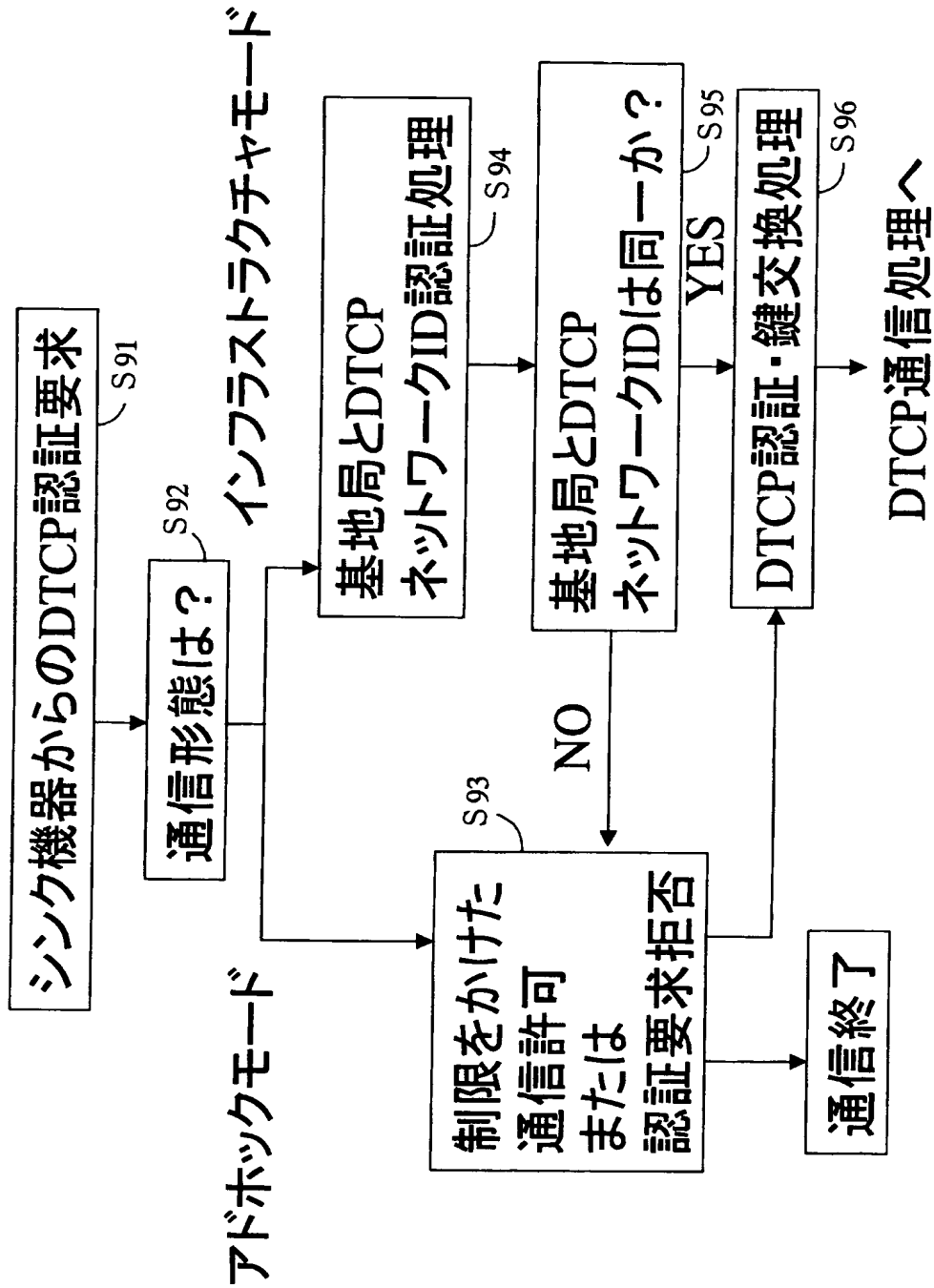


【図 1 7】





【図 1 8】



【書類名】 要約書

【要約】

【課題】 ユーザの使い勝手を悪くすることなく、著作権保護強化を図る。

【解決手段】 本発明に係る無線通信システムは、ローカルエリア無線ネットワーク A に接続されたソース機器 1、無線基地局 2 及びシンク機器 3 と、ローカルエリア無線ネットワーク B に接続されたソース機器 4 及び無線機器 5 とを備える。ソース機器 1 とシンク機器 3 で変更可能な DTCP ネットワーク ID の変更回数を制限するようにしたため、著作権保護を図る必要のあるコンテンツの悪用を防止できる。また、認証に失敗した場合に、コンテンツの送信を完全に禁止するのではなく、一定の制限をかけた上でコンテンツの送信を認めるようにしたため、著作権保護を図りつつ、ユーザの使い勝手を向上できる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 3 0 7 8 ]

|          |                    |
|----------|--------------------|
| 1. 変更年月日 | 2 0 0 1 年 7 月 2 日  |
| [変更理由]   | 住所変更               |
| 住 所      | 東京都港区芝浦一丁目 1 番 1 号 |
| 氏 名      | 株式会社東芝             |